Gestión Automática de incidentes e inventarios G.A.I.I.

Gibellini, Fabián[1]; Ruhl, Analía Lorena[2]; Di Gionantonio, M. Alejandra[3]; Rapallini, Marco[4]; Flores, Nora Viviana[5]; Serna, Mónica Mariel[6]

Laboratorio de Ingeniería en Sistemas de Información (LabSis)
Departamento de Ingeniería en Sistemas de Información
Universidad Tecnológica Nacional, Facultad Regional Córdoba (UTN-FRC)

([1])fgibellini@bbs.frc.utn.edu.ar; ([2])lruhl@bbs.frc.utn.edu.ar; ([3])ing.alejandradg@gmail.com; ([4])marco@bbs.frc.utn.edu.ar;([5])ingnoraflores@gmail.com; ([6])sernamonicam@gmail.com

Resumen

Uno de los problemas que enfrentan los grandes ambientes informáticos es conocer en tiempo real el parque informático del cual dispone, el estado de cada componente, las condiciones en las cuales se encuentran, y si están en reparación o desuso. [1] [2]

Actualmente, se han implementado algunas aplicaciones para inventariar los equipos y el software que forman parte del activo informático de diversos organismos. Estas aplicaciones permiten registrar en forma manual las distintas actualizaciones del inventario, ya sea por compras, bajas, reparaciones, etc.

Frente a esta problemática se diseñará una aplicación que permitirá implementar en forma automatizada el registro y control del inventario del hardware en cualquier establecimiento tanto público como privado, pero fundamentalmente, alertar ante el reemplazo y/o sustracción no autorizada de piezas en los equipos. Dicho Sistema de Alertas, será un subsistema del Sistema creado por el proyecto ya desarrollado durante período 2008-2010, Seguridad en Ambientes Informáticos (SAI)[3].

Palabras Claves

Sistema de Inventario, seguridad, notificaciones automáticas, tiempo real, sistema de alerta, almacenamiento de hardware, ambientes informáticos, seguridad en tiempo real.

Contexto

Esta aplicación se desarrolla en los laboratorios de la UTN Facultad Regional Córdoba de la Universidad Tecnológica Nacional, donde se realizarán las primeras pruebas sobre su funcionamiento. Inicialmente se implementará en las aulas del Laboratorio de Sistemas y luego se hará extensivo a los laboratorios de otras especialidades. Este Sistema de Inventario automatizado, será un subsistema del Sistema creado por el proyecto ya desarrollado en el mismo Laboratorio durante período 2008-2010, Seguridad en Ambientes Informáticos (SAI)[3]. El mismo, fue acreditado en la Facultad Regional Córdoba de la Universidad Tecnológica Nacional (Argentina), siendo ésta, la institución financiadora del proyecto. Código: EIPRCO757.

1. Introducción

Es prioritario en todo ambiente informático implementar normas de seguridad para resguardar los datos que en él se manejan, sin embargo, no podemos dejar de pensar en todo el equipo instalado que da soporte físico, como las estaciones de trabajo, servidores, computadoras personales y sus componentes. Por lo que en el Laboratorio de Ingeniería en Sistemas de Información de la Universidad Tecnológica Nacional Facultad Regional Córdoba, nos encontramos trabajando en un Proyecto de Seguridad integral que cubra todos los aspectos posibles de considerar sobre este tema.

Uno de los factores que impulsó a llevar a cabo este proyecto fue el creciente número de estudiantes que hacen uso de las instalaciones del Laboratorio de Ingeniería en Sistemas de Información, de la Universidad Tecnológica Nacional –Facultad Regional Córdoba, lo que demanda la instalación de nuevas computadoras, enlaces y diversos equipos. Frente a esta realidad, muy satisfactoria, se dificultan las tareasde los administradores y la cantidad de recursos que se deben controlar. [4][5]

El crecimiento constante de la plataforma tecnológica para cubrir esta realidad, requiere ser acompañadapor la implementación de un sistema integral de seguridad que permita conocer de manera sencilla y detectar el accionar de intrusos interesados en los componentes del hardware de los equipos del LabSis. El sistema GAII a desarrollar debe alertar ante cambios fuera de la configuración normal del hardware del equipo, reportando en tiempo real los cambios sufridos para una posterior revisión y toma de decisiones.

1.1 Integración con el sistema de Seguridad en Ambientes Informáticos (SAI)

El Sistema de Alertas, no es un sistema independiente, sino que el mismo es un subsistema que se integra al SAI. Este último, ya está desarrollado, y cuenta con tres subsistemas que conforman una suite de herramientas posibles de colaborar en la prevención y detección, sustracción y ataques a los equipos de un ambiente informático. Recordando que uno de los objetivos es lograr un sistema integral que sea de libre uso y de fácil acceso para cualquier organismo que lo requiera, haciendo hincapié en un sistema seguro y de muy bajo costo.

SAI está constituido por los siguientes subsistemas:

- Detección de Apertura de Gabinetes DAG [6].
- Sistemas alternativos de video vigilancia [7].
- Sistema Distribuido de Seguimiento Local y Remoto [8].

Este sistema integral SAI, a través de DAG permite detectar si se realiza la apertura de un dispositivo; el sistema de video vigilancia, permite el monitoreo a muy bajo costo; y el sistema remoto es la interfaz necesaria para el control de DAG.

Para optimizar y completar esta suite de herramientas, desarrollaremos una aplicación que permitirá obtener información de todos los componentes con los que se cuenta y mantenerlos actualizados de modo automatizado, apuntando a la posibilidad de alertar ante el reemplazo de alguno de ellos. Esta herramienta será escalable ya que no hay limitaciones en la cantidad de componentes a monitorear.

2. Líneas de Investigación y Desarrollo

El método utilizado para el presente trabajo de investigación está basado en el método empírico, de orientación cuantitativa observacional en la toma, análisis y

asociación de los datos cuantitativos arrojados por las aplicaciones bajo estudio. Pues, la informática utiliza los métodos empíricos, que toman conocimiento del objeto el uso de la experiencia [9]. Por tal motivo decidimos utilizar **OCS Inventory (Open Computer and Software Inventory)**[10]**,** el cual es un software libre que se publica bajo la GNU GPLv2[1], OCS-NG[2] recopila información sobre el hardware y software de equipos que hay en la red que ejecutan el programa de cliente OCS ("agente OCS de inventario"). Para analizar la forma de trabajo de la aplicación y determinar de qué manera nos servirán los datos que ésta nos entrega, instalamos la máquina virtual que se encontraba en la página oficial de OCS INVENTORY REPORT, "OCS-NG-Server-2.0.5-Debian-6.0.4-32bits.tar.gz" [11], la cual se ejecuta desde la aplicación VirtualBox [12].

3. Resultados y Objetivos

Los resultados obtenidos hasta el momento, luego de realizar todas las pruebas pertinentes dieron satisfactorias; en cuanto a la aplicación que se utilizará para desarrollar el módulo de alertas, el Sistema OCS ha sido la herramienta seleccionada para nuestro sistema.

El sistema GAII tomará los datos referente al hardware de la base de datos provista por el OCS-Server para generar un historial de inventarios, el cual nos proporcionará la información necesaria para generar reportes de manera automática de los cambios detectados en el hardware de la red.

[1]GNU GPLv2 (GNU: Is Not Unix)(GPL: General Public License)
[2] OCS-NG (Open Computer and Software Inventory Next Generation)

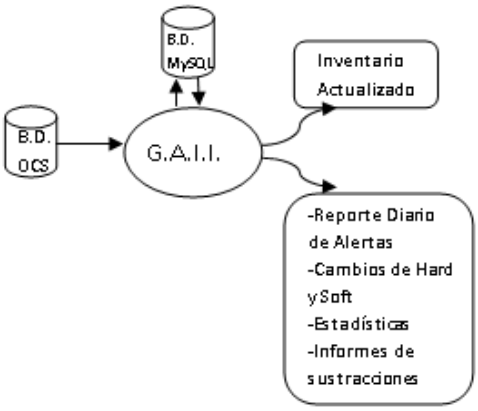

Fig. 1 Esquema básico del Sistema de Gestión Automática de incidentes e inventarios G.A.I.I.

Objetivo General:

Detectar y generar alertas sobre cambios y/o reemplazos no autorizados del hardware en equipos de computación, ubicados en aulas informáticas y ambientes públicos y/o privados, que requieran de un sistema de seguridad de bajo costo y fundamentalmente, de poca inversión inicial.

Objetivos Particulares:

- Brindar información actualizada de cada dispositivo tecnológico presente en el sistema del Labsis.
- Informar sobre los cambios en los históricos.
- Generar alertas vía mails al personal designado, para recibirlo y actuar en consecuencia.
- Generar alertas en tiempo real, enviadas por mail a otros dispositivos móviles.
- Detectar y documentar el estado real de las piezas de las computadoras después de cortes de energía eléctrica, o situaciones semejantes.
- Generar reportes con información que sea relevante para la toma de decisiones de la institución.
- Generar intercomunicación con el Sistema DAG[6]
- Aportar los datos para facilitar la gestión eficiente de incidentes e

inventarios, logrando la generación y reglas de asociación [13]

El mismo, nos brindará diariamente un reporte actualizado del contenido de cada PC, con sus movimientos, enviará un mail al administrador o a la persona encargada del lugar con el detalle de la alerta del cambio de algún elemento o modificación del equipo, inclusive si éste ha sido cambiado de lugar sin autorización o notificación del cambio.

4. Formación de Recursos Humanos

Este proyecto contribuirá a la formación y crecimiento de la carrera de investigador de los integrantes del mismo.

Dentro de este último, se contempla la formación de alumnos de la carrera de Ingeniería en Sistemas de Información.

Por otro lado, se prevé la capacitación de alumnos becarios que formarán parte del equipo mientras el proyecto dure. De esta manera, se generará un grupo de trabajo importante que promocione este tema.

Vemos también la posibilidad de colaborar con el crecimiento profesional de los integrantes del grupo, los cuales se ven predispuestos a perfeccionarse continuamente.

El grupo está compuesto por: Director, Co-Director, dos profesores investigadores de apoyo, tres profesores aspirantes a incorporarse a la carrera de investigador y un estudiante investigador de la carrera de Ingeniería en Sistemas de Información.

5. Conclusión

Con el desarrollo e implementación de esta herramienta se espera obtener un producto de suma utilidad, tanto para el LabSis como para empresas privadas y/o públicas quepermita tener el control inmediato del hardware activo en la entidad y colaborar en la toma de decisiones y en la prevención, detección, sustracción y fallos de componentes de hardware.

Es importante destacar, que el sistema busca la integración de sistemas ya desarrollados e implementados y de sistemas que se encuentran en su etapa de desarrollo.

6. Referencias

[1] Shyyunn Sheran Lin, Gregory S. Thompson, Viren Malaviya, “Embedded approach for device inventory collection utilizing OS programmability” SSTG, Cisco Systems170 W Tasman Drive, San Jose, California, U.S.A.(sheranl@cisco.com, gst@cisco.com) IEEE 1M 2011 Cisco SystemsCisco.com

[2] N. D. Arnold and D. A. Dohan, “Connection-Oriented Relational Database of the APS Control System Hardware”

Argonne National Laboratory, Argonne, IL 60439, USA 2003

[3] Seguridad en Ambientes Informáticos (SAI).
http://www.jidis.frc.utn.edu.ar/papers/e7c362c8b5427c807ee23beab34d.pdf

[4] Raydel Montesino and Stefan Fenz

“Automation possibilities in information security management”
Information Security Department
University of Informatics Sciences (UCI)

Havana, Cuba, raydelmp@uci.cu

SBA Research and Vienna University of Technology, Vienna, Austria, sfenz@sba-research.org IEEE 2011

[5] Álvaro Herrero, Emilio Corchado, Paolo Gastaldo, Francesco Picasso, Rodolfo Zunino, "Auto-Associative Neural Techniques for Intrusion Detection Systems". Department of Civil Engineering University of Burgos C/ Francisco de Vitoria s/n, 09006 Burgos, Spain. Dept. of Biophysical and Electronic Engineering (DIBE)Genoa University Via Opera Pia 11a, 16145 Genoa, Italy. 2007

[6] Detección de Apertura de Gabinetes
http://www.cneisi.frc.utn.edu.ar/papers/b998c93b46bb857450dfc6a89a03.pdf

[7] Sistemas alternativos de video vigilancia
http://www.cneisi.frc.utn.edu.ar/papers/b998c93b46bb857450dfc6a89a03.pdf

[8] Sistema Distribuido de Seguimiento Local y Remoto.
http://www.frsf.utn.edu.ar/cneisi2010/archivos/10-Sistema_Distribuido_de_Seguimiento_Local_y_Remoto.pdf
http://laboratorios.fi.uba.ar/lie/Revista/Articulos/020205/A2ago2005.pdf

[9] Barchini, G. Métodos "I+D" de la Informática. Universidad Nacional de Santiago del Estero, Argentina. 2005.
http://laboratorios.fi.uba.ar/lie/Revista/Articulos/020205/A2ago2005.pdf

[10] OCS Inventory Reports
http://www.ocsinventory-ng.org/

[11] OCS Inventory
http://www.ocsinventory-ng.org/en/download/download-server.html
http://wiki.ocsinventory-ng.org/index.php/Documentation:Main

[12] VirtualBox
www.virtualbox.org

[13] Uso de herramienta libre para la generación de reglas de asociación, facilitando la gestión eficiente de incidentes e inventarios
http://www.41jaiio.org.ar/sites/default/files/7_JSL_2012.pdf