Inventario seguro con alertas automáticas en ambientes informáticos de activos TI (I.S.A.)

Arias, Silvia Edith; Gibellini, Fabián; Ruhl, Analía Lorena; Di Gionantonio, M. Alejandra; Flores, Nora Viviana; Serna, MónicaMariel; Arch Daniel Félix; Zea Cárdenas, Milagros; Parisi, Germán; Barrionuevo, Diego

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

Resumen

Actualmente, diversos organismos que poseen una gran plataforma de dispositivos en su red, se encuentran con la problemática de llevar un inventario actualizado e informatizado, que les permita mantener la trazabilidad de éstos; lo complejo es la generación de alertas automáticas a los continuos cambios. La idea de resolver lo antes mencionado se gestó en uno de los laboratorios de la universidad, frente a la necesidad de tener control sobre el hardware instalado en los gabinetes de clases y laboratorios de investigación. De acuerdo con la exhaustiva exploración realizada sobre las aplicaciones propietarias y de código abierto que permiten inventariar y/o administrar el hardware de un sistema informático disponibles en mercado a la fecha, y luego de analizar las prestaciones de las mismas comparándolas y adecuándolas a los requerimientos del proyecto de investigación, se decidió utilizar los datos obtenidos por una aplicación de código abierto y libre disposición como soporte para la generación de las bases de datos que utilizará el subsistema a desarrollar, pues ésta permite visualizar el inventario a través de una interfaz web, pero no llevar registros sucesivos de la información que genera, es decir no genera un historial del hardware inventariado. Se trabajó en máquinas virtuales con sistemas operativos y software GNU necesarios para las pruebas, y sustentando el estudio con el empleo del método empírico. Este desarrollo, que será escalable, se integrará para optimizar y completar una suite de herramientas que ya funcionan en el laboratorio. El propósito es lograr un sistema integral, vía web, que sea de libre uso y de fácil acceso para cualquier organismo que lo requiera, haciendo hincapié en brindar un sistema seguro y de

muy bajo costo, que genere alertas automáticas y registro de historial, contribuyendo al desarrollo de recursos humanos específicos en éstas temáticas por un lado, y por el otro colaborar a la seguridad, principalmente en las instituciones públicas del país donde generalmente se sufre sustracciones indetectables por parte de intrusos. Esto responde a que la aplicación permitirá el monitoreo para generar alertas automáticas del activo informático de estos entes en forma gratuita; al tratarse de un software de código abierto, todo aquel que desee implementar el sistema podrá acceder a la aplicación y su código, como así también adaptarlo para la estructura del ambiente informático sobre el cual lo desee trabajar.

Palabras claves: seguridad, inventario, alertas automáticas

1. Introducción

"Un Sistema Informático está constituido por un conjunto de elementos físicos (hardware), lógicos (sistemas operativos, aplicaciones, etc.) y con frecuencia se incluyen también los elementos humanos (personal experto que maneje el software y el hardware)" (Aguilera López, 2010: 91-140).

En todo ambiente informático es prioritario 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 a los datos y que además es un activo importante para un organismo o empresa, como son: los servidores, las estaciones de trabajo, computadoras personales y sus componentes [2] [3]. Existen en el mercado aplicaciones desarrolladas para sistemas propietarios con licencias pagas que brindan información actualizada del parque informático en un ambiente TI, como VEO Ultimate compatible con Windows 7 que utiliza MySQL[4], Total Network Inventory 1.6 [5], HP Discovery and DependencyMappingInventory (DDMI) [6], ServiceDesk Plus 8.1 [7], y aplicaciones libres como lo son el OCS InventoryReport [8], FusionInventory[9], Open-AudIT (ComunityVersion)[10], ITDB[11], y GLPI [12], y otras con implementación de seguimiento satelital de laptops o PC en caso de robo, por ejemplo Lenovo en su línea ThinkPad con tecnología AntiThief provisto por Intel [13], posee un sistema de seguridad y administración embebido directamente en el chip que permite el control remoto interactivo de la computadora y su información.

I.S.A se gestó en el Laboratorio de Sistemas de Información (LabSis), de la Universidad Tecnológica Nacional – Facultad Regional Córdoba (U.T.N. – F.R.C), frente a la necesidad de tener un control del hardware instalado en los gabinetes de clases e investigación, debido a que en los últimos años, este parque informático ha tenido un incremento importante, impulsado por el creciente número de estudiantes que hacen uso de las instalaciones por un lado, y por los distintos convenios que la universidad tiene con empresas internacionales, por otro.

El sistema de inventario seguro con alertas automáticas, en ambientes informáticos sobre activos TI (I.S.A.), formará parte de un Sistema de Seguridad Automática e Integral, denominado S.A.I. [14]. Este último, ya está desarrollado y funcionando en el Laboratorio de Sistemas del Departamento Ingeniería en Sistemas de Información, cuenta con tres subsistemas que conforman una suite de herramientas posibles de colaborar en la prevención, detección, sustracción y ataques a los equipos de un ambiente informático.

SAI está constituido por los siguientes subsistemas:

- Detección de Apertura de Gabinetes DAG [15].
- Sistemas alternativos de Video Vigilancia [16].
- Sistema Distribuido de Seguimiento Local y Remoto [17].

El S.A.I., a través de D.A.G. 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.

2. Objetivos

Obtener un sistema integral, vía web, que sea de libre uso y de fácil acceso para cualquier organismo que lo requiera, haciendo hincapié en brindar un sistema seguro y de muy bajo costo, que genere alertas automáticas y registro de historial; que permita controlar, reportar, prevenir, proteger y tomar decisiones en tiempo y forma sobre el activo TI de cualquier institución que decida implementarlo.

Objetivos del Sistema I.S.A

- Mantener la trazabilidad de activos de TI, con un reporte diario actualizado del contenido de cada computadora y sus respectivos movimientos, enviando un mail al administrador o a la persona encargada con el detalle y la alerta de cambio de elemento o modificación de equipo, si la hubiere.
- Mantener una base de datos actualizada con el registro de cambios y/o novedades que detecte esta aplicación.
- Brindar información actualizada de cada dispositivo de hardware presente en las redes.
- Detectar y documentar los componentes de las computadoras después de cortes de energía eléctrica, o eventos similares inesperados.
- Generar informes estadísticos sobre cambios de hardware ocurridos en los equipos, y reportes con información relevante para la toma de decisiones en la Institución a partir de los datos históricos que almacenará el sistema.
- Interactuar con el Sistema de Detección de Apertura de Gabinete (DAG) para el intercambio de información relevante.

3. Metodología

La metodología utilizada en este proyecto de investigación es sobre la base de un método empírico de orientación cuantitativa observacional en la toma, análisis y asociación de los datos cuantitativos arrojados por las aplicaciones bajo estudio [18], [19]. Pues, la informática utiliza los métodos empíricos, que toman conocimiento del objeto mediante el uso de la experiencia. Se han realizado estudios exploratorios sobre las siguientes aplicaciones de código abierto:

- FusionInventory, el cual es un agente capaz de recuperar toda la información de todos los agentes instalados en las máquinas a inventariar, recolecta y envía la información a un servidor, el cual puede ser GLPI (Gestionnaire libre de parcinformatique o Administrador libre de activos informáticos), OCS Inventory NG. Su desventaja está en que la aplicación no maneja servidor propio.
- OCS Inventory NG (Open Computer and Software InventoryNextGeneration) [20], es un software libre que se publica bajo la licencia GNU GPLv2, el cual permite inventariar equipos informáticos activos en forma automática. Es soportado por la mayoría de los sistemas actuales en el mercado: Windows, Linux, MacOS, Sun Solaris, IBM AIXs y BSD, incluso hasta Android.
- Open-AudIT (ComunityVersion) es una aplicación web que sirve para obtener y mantener un historial de todos los recursos informáticos que se encuentran en una intranet: computadoras con sistema operativo Windows o Linux, Switches, Routers, Impresoras, Scanners, y cualquier dispositivo en la red que tenga una dirección IP (número que identifica a cada dispositivo dentro de una red con protocolo IP). Esta versión no permite llevar registros sucesivos de los cambios hechos en los componentes de una computadora y es una solución de código abierto.
- ITDB, es una aplicación web de gestión de inventario de activos que se utiliza para almacenar información acerca de los bienes que se encuentran en entornos de oficina, con un enfoque en los activos de TI. Solo es compatible con sistemas posix (Sistemas Operativos Portables donde X corresponde a Unix y sus derivados).
- GLPI (Gestionnaire libre de parcin formatique por su nombre en Francés), es un sistema administrador de recursos de una red, el cual posee una interfaz administrativa amigable y de fácil manejo e implementación, cuyo objetivo principal es facilitar la gestión y solución de todas las posibles incidencias de aquellos problemas que necesiten la intervención de personal especializado y llevar

un seguimiento del mismo a través de contratos, documentos, reparaciones de hardware, diccionario y estadísticas. Es una aplicación basada en PHP, MySQL [21] y Apache.

El desarrollo de los programas se realizará teniendo en cuenta las normas CMM y ISO/IEC 12207 [22] / ISO/IEC 25000:2500 [23] e ISO 9001[24] para asegurar la mejor calidad posible y capacitar a los alumnos en las mejores prácticas de Ingeniería de Software. Se utilizarán Metodologías ágiles del tipo SCRUM (1986) [25] / XP (1996) [26] / DSDM (1995) [27], para el desarrollo del Software.

4. Análisis

De acuerdo con los resultados aportados por la investigación exploratoria, previamente realizada sobre las aplicaciones propietarias y de código abierto, que permiten inventariar y/o administrar el hardware de un sistema informático, disponibles hasta la fecha en el mercado se prosiguió con el análisis exhaustivo sobre cada una de las siguientes herramientas: GLPI y OCS Inventory NG.

Con el propósito de analizar e investigar cómo trabajan las citadas aplicaciones de código abierto y libre disposición, se utilizó como herramienta la aplicación VirtualBox de Oracle [28] ya que con la misma es posible crear máquinas virtuales e instalar sistemas operativos adicionales, llamados sistemas invitados, dentro de otro sistema operativo denominado anfitrión. Una vez creada una máquina virtual en VirtualBox, se instaló como sistema operativo la distribución Debian GNU/Linux 6.0 (Squeeze).

La aplicación OCS Inventory NG, Consta de dos módulos principales, OCS InventoryReport (SERVIDOR) y OCS InventoryAgent instalado en c/u de las equipos a monitorear (CLIENTE). OCS Inventory NG recopila información sobre el hardware y el software de equipos que ejecutan el programa de cliente OCS ("Agente OCS de inventario"), como también de los dispositivos que hay en la red. OCS puede utilizarse para visualizar el inventario a través de una interfaz web sencilla y de fácil manejo, pero no permite llevar registros sucesivos de la información que genera, es decir no permite generar un historial del hardware inventariado. Provee estadística acerca de las conexiones por día o el número de malas conexiones, sistemas operativos diferentes y más. Para llevar a cabo las pruebas con el GLPI, se descargó e instaló la versión 0.84.5.Para no ingresar los datos manualmente debido a que el ingreso de los mismos al sistema I.S.A.será

automático, se utilizó el OCS como medio de entrada de datos, por lo tanto se comenzó a trabajar con estas dos herramientas integradas. Actualmente GLPI puede tomar los datos de los equipos a inventariar (disco duro, bios, memoria RAM, placas de red, video o audio, entre otros) desde OCS Inventory. A este proceso de toma de datos se le llama sincronización. Los tiempos de sincronización pueden ser programables. Además permite guardar historiales de estados de cada computadora con los cuales se pueden obtener informes estadísticos. No genera alertas automáticas en respuesta a un cambio o retiro de algún hardware, aunque guarda un registro de los mismos y se debe analizar el detalle de la información para poder detectar que cambios ocurrieron.

5. Resultados

GLPI es una herramienta muy potente para la administración de un área técnica, debido a que su valor radica en la gestión de tickets de incidencias o peticiones de asistencia técnica y por ende, su base de datos contiene muchas más tablas que el OCS Inventory NG y de las cuales este sistema no se interesaría por casi ninguna de ellas. Los datos migrarían primero desde la base de datos del OCS hasta la de base de datos de GLPI y recién desde este punto al sistema I.S.A. Es posible utilizar los datos obtenidos por la aplicación OCS como soporte para la generación de las bases de datos, que utilizará la aplicación a desarrollar I.S.A., para cumplir con el objetivo de mantener un historial sobre los activos T.I., y generar en base a éste las alarmas y reportes correspondientes.

La información que se desprende del análisis exploratorio y exhaustivo se ve reflejada en la tabla 1:

Características deseables		OCS Inventory NG 2.1	Fusion Inventory	Open - AuIT (Versión Community)	GLPI (Help desk)
Componentes	Servidor	si	no	si	si
	Agente	si	si	no	no
Inventariado Automático de HW		si	no	no	no
Sistemas Operativos soportados por Agente	Windows	si	si	no	no
	Linux	si	si	no	no

Sistemas Operativos soportados por Servidor	Windows	si	no	si	si
	Linux/Unix	si	no	si	si
Historial de cambio en hardware		no	no	no	si
Alertas automáticas ante remplazos o/o retiros de hardware		no	no	no	no
Interfaz de Administración Web		si	si	si	si
Exploración de red e identificación de dispositivos desconocidos		si	no	si	no
Funciones de exportación de datos	CSV	no	no	si	si
	XLS	no	no	si	no
	XML	si	si	si	si
	PDF	no	no	no	si
Acceso remoto al servidor		si	no	no	si
Reportes/Estadísticas		si	no	si	si

Tabla 1. Características necesarias en el software para lograr la obtención de datos

6. Conclusión

Es posible utilizar los datos obtenidos por la aplicación OCS como soporte para la generación de las bases de datos que utilizará la aplicación a desarrollar I.S.A., para cumplir con el objetivo de mantener un historial sobre los activos T.I., y generar en base a éste las alarmas y reportes correspondientes.

Sobre la base de los estudios y pruebas mencionadas *ut supra* se selecciona la aplicación OCS como adecuada y pertinente para desarrollar el sistema I.S.A., esto debido a que los resultados de las referenciadas pruebas fueron satisfactorios y que de los mismos estudios se desprende que la aplicación OCS, se adapta a los requerimientos del sistema a desarrollar.

Referencias bibliográficas

[1] Aguilera Lopez, Purificación (2010) , “Seguridad Informática” , Madrid, Editorial Editex, S.A. Briand, L. C., Daly, J., and Wüst, J., "A unified framework for coupling measurement in objectoriented systems", *IEEE Transactions on Software Engineering*, 25, 1, January 1999, pp. 91-121.

[2] Shyyunn Sheran Lin, Gregory S. Thompson, Viren Malaviya. (2011). “Embedded approach for device inventory collection utilizing OS programmability” SSTG, Cisco Systems170 W Tasman Drive, San Jose, California, U.S.A

[3] N. D. Arnold and D. A. Dohan.(2003) “Connection-Oriented Relational Database of the APS Control System Hardware Argonne National Laboratory, Argonne, IL 60439”.USA .

[4]VEOUltimate. Consulta en línea en:http://www.veo.com.mx/funciones/inventariohw.html

[5] Total Network Inventory 1.6 http://www.manageengine.com/products/service-desk/asset-inventory-management.html

[6]HP Discovery and Dependency Mapping Inventory (DDMI). http://www8.hp.com/lamerica_nsc_cnt_amer/es/software/software-product.html?compURI=tcm:237-936991

[7] Service Desk Plus http://www.manageengine.com/products/service-desk/asset-inventory-management.html?gclid=CNdtL2i5bICFQTnnAodiTgAqA

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

[9] FusionInventoryhttp://www.fusioninventory.org/overview/index.es.html

[10] Open-Audit http://www.open-audit.org/

[11] ITDB http://www.sivann.gr/software/itdb/

[12] GLPI http://www.glpi-project.org/

[13] Lenovo ThinkPad http://www.fasanar.com/tag/intel/

[14]Seguridad en Ambientes Informáticos (SAI).
http://www.jidis.frc.utn.edu.ar/papers/e7c362c8b5427c807ee23beab34d.pdf
[15]Detección de Apertura de
Gabineteshttp://www.cneisi.frc.utn.edu.ar/papers/b998c93b46bb857450dfc6a89a03.pdf
[16]Sistemas alternativos de video vigilancia
http://www.cneisi.frc.utn.edu.ar/papers/b998c93b46bb857450dfc6a89a03.pdf
[17]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
[18] Bunge, M. (1998). *La ciencia su Método y su Filosofía*. Buenos Aires: Editorial Siglo Veinte.
[19] Barchini. (2005). G. *Métodos "I+D" de la Informática.* Universidad Nacional de Santiago del Estero, Argentina.
[20] OCS Inventory http://wiki.ocsinventory-
ng.org/index.php/Documentation:Administrationhttp://wiki.ocsinventory-
ng.org/index.php/Documentation:Exportinv http://wiki.ocsinventory-
ng.org/index.php/Documentation:OCSsynchroLDAP
[21] Learning PHP, MySQL, JavaScript, CSS & HTML5: A Step-by-Step Guide to Creating Dynamic Websites by Robin Nixon (Author) June 16, 2014 Edition: 3rd
[22] www.iso.org
[23] http://iso25000.com
[24] NORMA ISO 9001(2000). Calidad en el desarrollo de software.
[25] Alonso Alvarez Garcia, 2012, METODOS AGILES Y SCRUM. ANAYA MULTIMEDIA.
[26] Letelier P., Penadés C., Metodologías ágiles para el desarrollo de Software: eXtreme Programming (XP), Universidad Politécnica de Valencia. Disponibleen:
http://www.willydev.net/descargas/masyxp.pdf
[27] Steven Kelly and Juha-Pekka Tolvane. (2008) Domain-Specific Modeling: Enabling Full Code Generation. Wiley-IEEE Computer Society Press.
[28] Máquina virtual VirtualBox . Disponible en línea : https://www.virtualbox.org/