Integración de un panel de alarma de incendio y un sistema de cámaras de vigilancia IP con la consola de seguridad informática OSSIM

Juan David Osorio Betancur

Luis Ernesto Cárdenas

Rodrigo Bedoya

Cristian Latorre

Juan Manuel Madrid Molina

Fecha de recepción: 5-03-2008 Fecha de selección: 24-10-2008 Fecha de aceptación: 15-9-2008

ABSTRACT

Security consoles are among the most widely deployed tools for enterprise-wide information security management. In order to assure an optimal coverage of the information security requirements according to international standards, security consoles should take into account the physical security domain. This article summarizes the work of our research team, in order to integrate a fire alarm control panel and an IP surveillance camera system with the OSSIM information security console.

KEYWORDS

Information security, physical security, security consoles, OSSIM, fire alarms, CCTV systems.

RESUMEN

Una de las herramientas más usadas hoy en día para la gestión de la seguridad informática en las empresas es la consola de seguridad. Para garantizar un cubrimiento óptimo de los requerimientos de seguridad informática enunciados en normas internacionales, las consolas de seguridad deberían tener en cuenta el dominio de la seguridad física. Este

artículo resume el trabajo efectuado por nuestro equipo de investigación para integrar un panel de alarma contra incendio y un sistema de cámaras de vigilancia IP con la consola de seguridad informática OSSIM.

PALABRAS CLAVE

Seguridad informática, seguridad física, consolas de seguridad, OSSIM, alarmas contra incendio, sistemas de CCTV.

Clasificación Colciencias: Tipo 1

INTRODUCCIÓN

La gestión de la seguridad informática se ha convertido en una necesidad para las organizaciones de hoy, debido a exigencias legales[1,2] y de cumplimiento con estándares internacionales.[3,4]

Una de las herramientas más útiles en dicha labor es la consola de gestión que recoge información de los diferentes equipos y redes que conforman la plataforma informática de la organización, con el fin de detectar configuraciones y/o eventos que podrían considerarse como una amenaza o una evidencia de ataque informático, y de esa manera poder reaccionar oportunamente y mantener la información en un estado seguro. La consola de gestión también permite obtener estadísticas e informes acerca del estado de seguridad de los sistemas de la organización, que se pueden emplear para verificar el cumplimiento de indicadores de gestión.

Una de las consolas de gestión de código abierto más populares en la actualidad es OSSIM.[5] Esta consola, además de recolectar y uniformizar los eventos de los diferentes sistemas, correlaciona los eventos que ocurren en el sistema en análisis, con el fin de minimizar el número de alertas que el administrador recibe y eliminar falsos positivos.

En la actualidad, OSSIM es capaz de recolectar información acerca de una gran cantidad de eventos relacionados con seguridad lógica. Sin embargo, hasta el momento no se ha integrado en el sistema la capacidad de recolectar información acerca del entorno físico,[6] que es otro de los grandes dominios de la seguridad informática.[3]

Este artículo describe el trabajo realizado por nuestro equipo investigador, para posibilitar la captura de eventos del entorno físico en OSSIM. Particularmente, se documenta el desarrollo de interfaces para capturar información desde un panel de alarma de incendio, y desde un sistema de monitoreo de cámaras de seguridad IP. Se inicia con un panorama de la seguridad informática, y de la problemática que busca ser resuelta por las consolas de seguridad. Luego se hace una descripción general de la arquitectura de OSSIM. Se continúa con una justificación de la inclusión de dispositivos físicos en el entorno de OSSIM, desde el punto de vista de buenas prácticas en seguridad informática. Acto seguido se describen las interfaces creadas, y se cierra con un apartado de conclusiones.

Problemática de gestión de la seguridad informática

Para que un sistema informático se considere como seguro, debe cumplir con cuatro premisas básicas:[7]

- La información que contiene debe ser confidencial, es decir, no debe poder ser consultada por terceros que no deberían tener en principio acceso a ella.
- De igual manera, dicha información debe conservar su integridad, o sea no dañarse o alterarse a medida que se mueve por el sistema
- El sistema debe ser capaz de autenticar a sus usuarios y a la información que recibe, de tal manera que la fuente de la infor-

mación siempre sea verificable, y que solamente los usuarios autorizados puedan acceder al sistema.

- El sistema debe estar disponible cuando se lo necesite.

Un ataque informático atenta contra una o varias de estas premisas. Como se puede ver, la labor del oficial de seguridad de un sistema informático no es nada fácil, ya que continuamente se pueden presentar ataques que aprovechen vulnerabilidades existentes o nuevas. La seguridad absoluta no existe, porque a medida que se descubren nuevas vulnerabilidades y se solucionan, dichas soluciones pueden introducir otras vulnerabilidades, o el avance de la tecnología hace que sistemas que antes se consideraban como seguros pasen a ser vulnerables, debido al descubrimiento de nuevos métodos de ataque.

Por otro lado, la legislación de los diferentes países se ha ido actualizando con el fin de castigar el delito informático, pero a la vez exige que se disponga de un nivel adecuado de protección en los sistemas de información.[1,2] La seguridad de la información también se ha convertido en asunto crítico para procesos de calidad total de las empresas y estrategias de gobierno de tecnologías de información. En todos estos procesos no solamente se exige que existan mecanismos que garanticen la seguridad,[3] sino que se requiere cuantificar su impacto mediante el uso de indicadores.[4]

Existen diversas herramientas que pueden ayudar al administrador en la tarea de mantener seguro un sistema informático. Dichas herramientas se pueden clasificar en los siguientes grupos:

- **Antivirus**: Se encargan de detectar y eliminar software maligno de un sistema informático. Dependiendo de su funcionalidad, también pueden controlar los diferentes vectores de infección (correo electrónico, medios de almacenamiento removibles, etc.).
- **Detectores de intrusos basados en host (HIDS, Host-based Intrusion Detection Systems)**: Este tipo de software monitorea procesos y archivos críticos del sistema en análisis, y reporta cuando se producen cambios que puedan considerarse como evidencia de un ataque informático.
- **Detectores de intrusos basados en red (NIDS, Network-based Intrusion Detection Systems)**: Los NIDS revisan continuamente los datos que circulan por la red, y avisan cuando observan tráfico que evidencia un ataque o una tentativa de ataque informático.
- **Firewalls**: Un firewall actúa como aislador entre el tráfico de la internet y el tráfico interno de la red corporativa. Mediante un conjunto de reglas determina qué paquetes pueden pasar o no a través de él, y registra las violaciones a dicha política.
- **Detectores de vulnerabilidades**: Estos programas hacen un análisis detallado de un sistema de cómputo, y arrojan como resultado las vulnerabilidades que existen en el sistema operativo y el software instalado. Hay dos

tipos de detectores de vulnerabilidades: Los basados en red, que hacen el análisis del equipo en forma remota a través de la red; y los basados en host, que se ejecutan directamente sobre el equipo a analizar.

La abundancia de herramientas, y el hecho de que deban emplearse varias de ellas en conjunto para monitorear los diferentes frentes del sistema informático, trae consigo varios problemas graves:

- Falta de uniformidad en el formato de los registros de actividad. Cada herramienta emplea un formato diferente para reportar las alertas de seguridad, obligando de este modo al administrador a conocerlos todos.
- Exceso de alertas. En sistemas grandes, o con actividad alta, el número de alertas que se genera en un determinado período puede exceder la capacidad de trabajo del administrador.
- Manejo de falsos positivos. Dependiendo de la configuración de las herramientas, pueden reportarse como alertas de seguridad eventos que son, en realidad, parte del funcionamiento habitual del sistema.

En un escenario como este se hace necesario contar con una herramienta que permita unificar y centralizar la gestión de las alertas de seguridad. Las herramientas de esta naturaleza se denominan consolas de seguridad. A continuación, se hará una breve descripción de OSSIM, que es la consola de seguridad empleada en nuestro proyecto de investigación.

Generalidades y arquitectura de OSSIM

La plataforma OSSIM (Open System Security Information Management)[5] es una consola de seguridad de código abierto, de amplio uso en la actualidad. Tiene la capacidad de consolidar alertas de una gran cantidad de sistemas de seguridad basados en código abierto, y es altamente configurable, de tal manera que permite procesar información de programas y dispositivos de seguridad. La arquitectura de OSSIM es distribuida y comprende cuatro elementos básicos.[8] (Figura1).

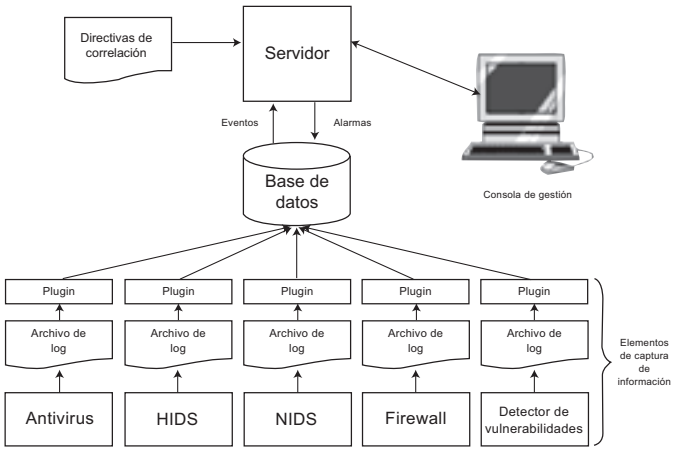

Figura 1. Arquitectura del sistema OSSIM

- **Elementos de captura de información**: Recolectan la información requerida por OSSIM, en los diferentes sitios del sistema informático en donde se desea hacer control. Virtualmente cualquier programa o dispositivo de seguridad informática puede servir como entrada al sistema OSSIM, siempre que sea capaz de generar archivos de bitácora (log) en formato de texto plano. La interfaz se hace escribiendo un archivo de configuración de plugin adecuado. Los plugins así configurados actúan como traductores de alertas, tomando el registro de la alerta en su formato nativo y traduciéndolo al formato estándar empleado por OSSIM. El elemento clave del archivo de configuración de plugin es la **expresión regular,**[6] que define la manera como puede encontrarse la información que OSSIM requiere en el archivo de log.
- **Base de datos**: Almacena todos los eventos recibidos de los diferentes elementos de captura de información, así como las alarmas generadas por el motor de correlación del servidor.
- **Servidor**: El servidor correlaciona los eventos registrados en la base de datos, con el fin de detectar patrones que evidencien una vulnerabilidad en el sistema o un ataque informático, y a la vez actúa como filtro para tratar de eliminar la mayor cantidad posible de falsos positivos. Para efectuar este proceso, OSSIM emplea una serie de directivas de correlación que deben ser personalizadas por el administrador del sitio para garantizar un óptimo funcionamiento. Una vez efectuada la correlación, una gran cantidad de eventos pueden consolidarse en una sola alarma, que se presenta por consola al administrador del sistema. Además, con base en las alarmas que se presenten y en el valor de importancia relativa que el administrador haya asignado a cada uno de los activos informáticos de la empresa, OSSIM es capaz de calcular también el nivel de riesgo informático del negocio.
- **Consola de gestión**: La consola es el front-end gráfico del sistema. Funciona vía web, y permite al administrador del sistema consultar las alarmas, reportes y estadísticas que genera el sistema.

Justificación de la inclusión del dominio de la seguridad física en OSSIM

La norma ISO 17799:2005[3] comprende once dominios que se deben tener en cuenta para el diseño de una política de seguridad informática. En la actualidad, OSSIM puede emplearse como tablero de control para monitorear el cumplimiento de políticas de seguridad, en los siguientes dominios:

- Administración de activos
- Administración de comunicaciones y operaciones
- Control de acceso
- Administración de incidentes de seguridad informática

Esto se debe a que la arquitectura actual de OSSIM se concentra en la recolección de información en la red y

los equipos de procesamiento de datos conectados a ella.

Sin embargo, debe notarse que los fabricantes de equipos para el control de seguridad física, tales como cerraduras, alarmas contra robo e incendio, cámaras de vigilancia, etc., incluyen cada vez con más frecuencia la opción de interfaz de red en dichos equipos. Siendo el dominio de la seguridad física de igual importancia que los otros diez, resulta lógico centralizar también la recolección de alertas provenientes de estos equipos. La arquitectura abierta de OSSIM posibilita el desarrollo de las interfaces necesarias para capturar dicha información.

En el desarrollo del proyecto de investigación "Adaptación y mejoras al motor de correlación y sensores remotos del sistema OSSIM para un centro de seguridad informática", acometido por la Universidad Icesi y Sistemas TGR, S.A., se propuso como uno de los cinco objetivos a lograr la integración de una alarma de incendio y de una cámara IP de vigilancia a OSSIM. En los apartados siguientes se documenta la manera cómo se hizo la integración, empleando software libre de código abierto.

Integración de OSSIM con una alarma de incendio

Todo centro de cómputo debería contar con un sistema adecuado de protección contra incendios, de acuerdo con la norma ISO 17799:2005. Los paneles de alarma de incendio son muy convenientes en este entorno, ya que centralizan la recepción de las señales de alarma, dan la alerta necesaria para proteger al personal, y en caso de que así se configuren, pueden controlar la fase inicial de extinción del incendio.

La mayoría de los paneles de alarma de incendio existentes en el mercado tienen la posibilidad de conectarse a una central de monitoreo remoto, empleando una línea telefónica. Una vez conectado, el panel transmite los datos de la alerta a la central, empleando una secuencia de tonos DTMF. El protocolo más usado para este propósito fue desarrollado por Ademco (hoy parte del grupo Honeywell), y se le conoce como Contact ID.[9] Dicho protocolo fue elevado a nivel de estándar en 1999 por la SIA (Security Industry Association),[10] entidad que agrupa a la mayoría de fabricantes de equipos de seguridad. De hecho, el protocolo Contact ID es empleado no solamente por paneles de alarma contra incendios, sino también por paneles de alarma contra ladrones y otros dispositivos de seguridad habilitados para reportar eventos a centrales de monitoreo.

La solución concebida para integrar un panel de alarma al sistema OSSIM se ilustra en la Figura 2.

Se empleó un panel de alarma LYNXR de Honeywell[18] para las pruebas. La salida telefónica del panel de alarma se conectó a un servidor Linux, dotado con una tarjeta FXO/FXS Digium TDM11B para manejo de voz sobre IP,[11] y el software Asterisk, que implementa un PBX IP.[12] Seguidamente, se configuró bajo Asterisk el puerto FXS de la tarjeta con un número de extensión, y el panel de alarma para que marcara dicho número de extensión en el momento en que requiera reportar algún evento.

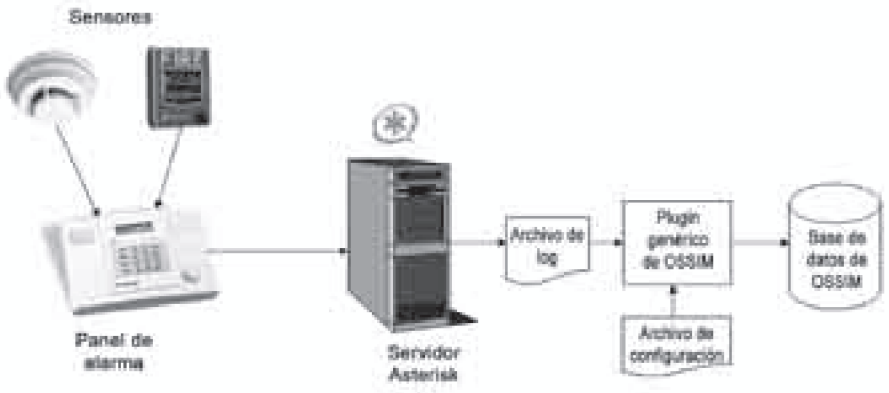

Figura 2. Integración de un panel de alarma de incendio con el sistema OSSIM

La extensión se configura en Asterisk para que conteste automáticamente después de un cierto número de timbres, y para que ejecute la función AlarmReceiver() una vez conteste. AlarmReceiver()[13] es una rutina incluida con la distribución de Asterisk, que se encarga de recibir la secuencia de tonos DTMF enviada por el panel de alarma, decodificarla, y escribir el registro de la alarma en un archivo de log.

El registro de la alarma contiene la siguiente información:[9]

- Un código de cuatro dígitos que identifica el panel en forma única
- Tipo de mensaje: Consiste siempre en los dígitos 18 ó 98, que especifican que el mensaje es del protocolo Contact ID.
- Calificador de evento: Número de un solo dígito, igual a 1 si se está anunciando un evento nuevo, 3 si se está anunciando que un evento previo dejó de ocurrir, o 6 si se desea reportar que una condición o evento previo persisten.
- Código del evento: De tres dígitos. El primer dígito, entre 1 y 6, especifica el tipo de evento (alarma, problema interno del sistema, activación/inactivación, etc.).
- Número de la partición o grupo: Código de dos dígitos. Las particiones se emplean por lo regular cuando se desea monitorear varios edificios o sitios separados, utilizando un solo panel de alarma. En este caso se configura en la alarma una partición por cada edificio o sitio.
- Número de la zona: Código de tres dígitos. Identifica al sensor o usuario que generó el evento.
- Un dígito de checksum.

Se procedió entonces a diseñar un archivo para configuración del plugin genérico de OSSIM. El plugin convierte cada registro al formato estándar empleado por OSSIM, y registra la información en la base de datos. Además, define una tabla que permite traducir los códigos numéricos de evento a cadenas de texto más descriptivas. El administrador del

sitio puede optar también por crear tablas de conversión en el mismo archivo, para traducir los códigos de partición y los códigos de zona.

De esta manera, fue posible lograr que OSSIM registrara eventos generados por cualquier panel de alarma compatible con el protocolo Contact ID.

Integración de OSSIM con cámaras IP de vigilancia

De acuerdo con la norma ISO 17799:2005, debe existir un perímetro de seguridad física en toda instalación que contenga equipos de procesamiento de datos, así como sistemas que detecten la presencia de intrusos dentro de dicho perímetro. Los sistemas de circuito cerrado de televisión (CCTV) han sido empleados por muchos años para este propósito en áreas que así lo requieren, tales como bancos, almacenes, centros comerciales, viviendas, etc.

Una de las grandes desventajas de estos sistemas en el pasado era la necesidad de supervisión continua de los monitores conectados a las cámaras, con el fin de poder detectar a tiempo un acceso no autorizado a determinada área. En caso de no haber nadie presente supervisando los monitores, era posible revisar posteriormente la grabación para encontrar evidencia del acceso no autorizado.

En la actualidad, los sistemas de grabación digital (Digital Video Recorders, DVR) permiten, además de almacenar el video capturado por las cámaras, procesarlo mediante algoritmos de detección de movimiento.[14] Se pueden entonces demarcar zonas dentro del campo de visión de las cámaras, de tal manera que si el algoritmo de detección de movimiento observa cambios en alguna de dichas zonas, notifique del evento al operador. El sistema de grabación procede también a marcar la sección del video en la que se detectó el movimiento para facilitar su posterior consulta.

Los algoritmos de detección de movimiento pueden ejecutarse en el DVR o en las cámaras conectadas. La primera opción permite emplear cualquier tipo de cámara de vigilancia, pero cada cámara adicional que se conecte al DVR consumirá cierta capacidad de procesamiento, por lo cual debe tenerse cuidado de no sobrecargar el sistema. La segunda opción exige que se empleen cámaras especiales más costosas, pero se descarga al DVR del procesamiento adicional, pudiendo entonces conectarse más cámaras al sistema.

ZoneMinder[15] es una solución de código abierto, que permite implementar un sistema de monitoreo de cámaras de vigilancia con funciones de DVR en el sistema operativo Linux. Admite conexión de cámaras de vigilancia mediante tres opciones: tarjeta de captura de video, puerto USB e interfaz de red (para el caso de cámaras IP). La arquitectura de ZoneMinder se puede apreciar en la Figura 3.

Los componentes de la arquitectura se describen brevemente a continuación.[16]

- **El demonio de captura (zmc)** se conecta al dispositivo de la cámara y captura el flujo de video de la misma. Normalmente se configura un demonio de captura por cada cámara conectada al sistema.

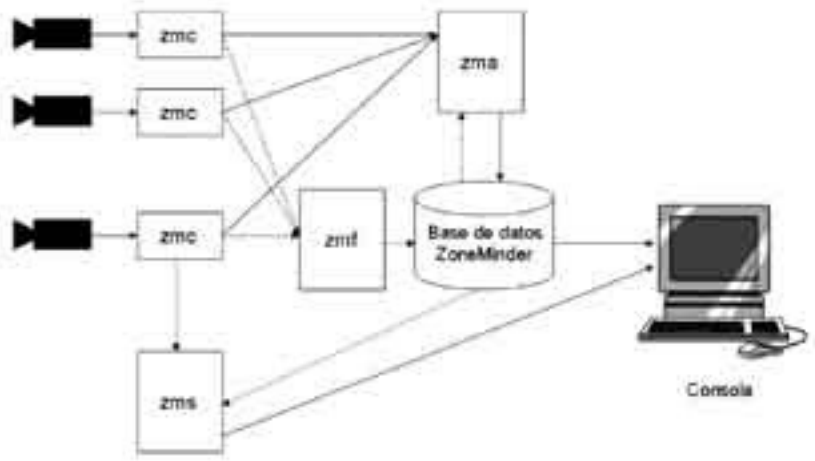

Figura 3. Arquitectura de ZoneMinder

- **El demonio de análisis (zma)** analiza los flujos de video provenientes de las cámaras y aplica el algoritmo de detección de movimiento. En caso de encontrar movimiento, se encarga también de almacenar el segmento de video que ocasiona el evento, y registrar dicho evento en su base de datos.
- **El demonio de almacenamiento de cuadros (zmf)** se puede configurar en forma opcional, en caso de que el volumen de datos proveniente de las cámaras sea muy alto. Cuando se configura zmf, éste se encarga de almacenar los flujos de video en un dispositivo de almacenamiento secundario, desde donde el demonio zma puede leerlos y procesarlos posteriormente.
- **El servidor de streaming (zms)** se activa cuando el usuario final desea ver un flujo de video en vivo de una cámara en particular, o un flujo de un evento. Se encarga de transmitir el video al navegador web del usuario.
- **La consola** es una interfaz web basada en PHP, que permite administrar las diferentes opciones del software, configurar las cámaras y observar los videos, bien sea los flujos en vivo de las cámaras, o las secuencias capturadas como consecuencia de un evento.

ZoneMinder permite definir una entidad llamada **monitor** por cada cámara que se desee monitorear. Dicho monitor puede operar en cuatro modalidades:

- **Solo monitoreo**: No efectúa detección de movimiento, solamente permite conectarse a la cámara para obtener su flujo de video.
- **Detección de movimiento**: Todo el video capturado se analiza, y se generan eventos cuando se registra movimiento en las zonas configuradas en el monitor.
- **Grabación**: El flujo de video de la cámara se graba completo en

almacenamiento secundario. No se efectúa detección de movimiento.

- **Grabación y detección**: Se graba el flujo de video de la cámara, y cuando se detecta movimiento, la secuencia de interés se marca y se genera un evento.

En el momento de la creación de cada monitor se define una zona por omisión, que consiste en el cuadro completo que captura la cámara. De este modo, si se presenta movimiento en cualquier parte de la imagen, se genera un evento. Este no es normalmente el comportamiento deseado, por lo cual ZoneMinder permite saber cuáles zonas del cuadro generarán un evento cuando se presente movimiento en ellas, y cuáles no.

La Figura 4 ilustra la integración de ZoneMinder con el sistema OSSIM.

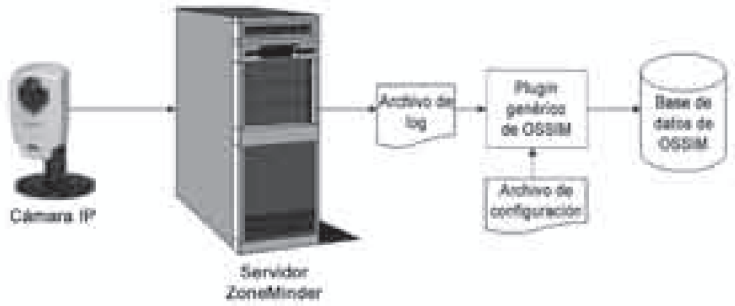

Figura 4. Integración de ZoneMinder con el sistema OSSIM

Como fuente de video se empleó una cámara IP Axis 207.[17] Se configuró un monitor de ZoneMinder sobre esta cámara; en las opciones de dicho monitor se especificó que debería generarse un registro, cada vez que ocurriera movimiento en alguna de las zonas configuradas. El registro que genera ZoneMinder en principio es muy limitado, puesto que solamente contiene la fecha, la hora y el nombre del monitor en el que se generó el evento. Se cambió entonces un parámetro de configuración de ZoneMinder para obligarlo a generar una mayor cantidad de información de depuración en los logs, con lo cual cada evento genera varios registros separados:

- Un registro de inicio del evento, que contiene el nombre del monitor donde se presentó.
- Un registro adicional por cada dos o tres cuadros de video donde se presente movimiento. Estos registros adicionales incluyen el nombre de la zona que generó el evento.

Logrado esto, se escribió un archivo de configuración para el plugin genérico de OSSIM. Este archivo de configuración es mucho más sencillo que el de la alarma de incendio, porque el registro del evento ya contiene el nombre del monitor y de la zona donde se generó el evento, de tal modo que no se requiere hacer traducción de códigos.

De esta manera se logró integrar un sistema de vigilancia basado en cámaras IP con OSSIM. En un futuro se desea modificar la consola forense de OSSIM, de tal manera que al seleccionar el evento generado por ZoneMinder, se abra la consola de ZoneMinder y se pueda ver el segmento de video que causó la alerta.

Conclusiones y trabajo futuro

La consola OSSIM presta un invaluable servicio al administrador de un sistema informático, brindándole información útil para la toma de decisiones en el campo de la seguridad informática. Considerando la importancia de la seguridad física en el conjunto de requisitos necesarios para poder tener un sistema informático, y con la intención de mejorar una herramienta de muy buena calidad, nuestro equipo investigador logró desarrollar las interfaces necesarias para integrar un panel de alarma de incendios y un sistema de cámaras de vigilancia IP a la consola OSSIM.

La solución implementada emplea en su totalidad software libre de código abierto, por lo cual preserva la filosofía original de OSSIM, y permite su implementación a un costo relativamente bajo.

La integración de OSSIM con el panel de alarma contra incendios trajo un valor agregado adicional al proyecto: la posibilidad de integrar a la consola cualquier dispositivo de seguridad que emplee el protocolo Contact ID para reportar eventos a una central. Dado el uso extendido de este protocolo, las posibilidades de integración con diferentes dispositivos de seguridad física son muy grandes.

Por su parte, la integración de OSSIM con el sistema de cámaras de vigilancia IP, mostró la posibilidad de emplear hardware económico y la infraestructura de red de datos de la empresa, para construir una solución de monitoreo físico confiable e integrada con los sistemas de seguridad informática.

En el marco del mismo proyecto de investigación, se está trabajando en un módulo que permite generar directivas personalizadas para el motor de correlación de OSSIM, mediante el agrupamiento (clustering) de las alertas que se registran en la base de datos. Asimismo, se está trabajando en un esquema para optimizar el funcionamiento de OSSIM en redes de muy alto tráfico, con el fin de evitar que se pierdan datos de alertas debido al alto volumen de alertas que se genera.

RECONOCIMIENTOS

Este trabajo de investigación fue financiado en parte por Colciencias y la Gobernación del Valle del Cauca, en el marco de la convocatoria 041/2007: "Concurso público de méritos para la financiación de proyectos basados en investigación, desarrollo tecnológico e innovación en el marco del fortalecimiento de la competitividad de las apuestas productivas estratégicas del Departamento del Valle del Cauca". Como entidad ejecutora del proyecto participó la Universidad Icesi, y como entidad beneficiaria, Sistemas TGR, S.A.

BIBLIOGRAFÍA

1. Unión Europea. Protección de datos en la Unión Europea. 2000.
   http://ec.europa.eu/justice_home/fsj/privacy/docs/guide/guide-spain_es.pdf .
   Descargado el 5-SEP-08
2. United Status Congress. Sarbanes-Oxley Act of 2002. 23 de enero de 2002.
   http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf .
   Descargado el 5-SEP-08
3. International Standards Organization (ISO). Information technology – Security techniques – Code of practice for information security management (Norma
   ISO/IEC 17799:2005). Junio de 2005. 115 pp.
4. International Standards Organization (ISO). Information technology – Security techniques – Information security management systems – Requirements (Norma ISO/IEC 27001:2005). Noviembre de 2005. 34 pp.
5. OSSIM (Open System Security Information Management).
   http://www.ossim.net
6. OSSIM: Agent Documentation.
   http://www.ossim.net/dokuwiki/doku.php?id=documentation:agent#plugins .
   Descargado el 5-SEP-08
7. Carracedo Gallardo, Justo. Seguridad en redes Telemáticas. McGraw-Hill, España, 2004. Capítulo 1, 1-32 pp.
8. Casal, Julio. OSSIM: General Description Guide.
   http://www.ossim.net/dokuwiki/doku.php?id=documentation:general_description .
   Descargado el 5-SEP-08
9. Security Industry Association. Digital Communication Standard - Ademco ® Contact ID Protocol - for Alarm System Communications.
   http://www.smartelectron.ru/files/DC-05_Contact_ID.pdf .
   Descargado el 5-SEP-08
10. Security Industry Association. http://www.siaonline.org/
11. Digium FXS / FXO cards.
    http://www.digiumcards.com/digium_cards_combos.html
    Descargado el 5-SEP-08
12. Asterisk – The Open Source PBX & Telephony Platform.
    http://www.asterisk.org
13. Asterisk Alarmreceiver - SIA (Ademco) Contact ID Alarm Receiver Application.
    http://www.voip-info.org/wiki/index.php?page=Asterisk+cmd+AlarmReceiver
    Descargado el 5-SEP-08
14. Axis Communications. Video Motion Detection (VMD).
    http://www.axis.com/products/video/about_networkvideo/vmd.htm
    Descargado el 5-SEP-08
15. ZoneMinder: Linux Home CCTV and Video Camera Security with Motion
    Detection. http://www.zoneminder.com/

16. ZoneMinder Main Documentation.

http://www.zoneminder.com/wiki/index.php/Main_Documentation

Descargado el 5-SEP-08

17. Axis Communications. Axis 207 Network Camera.

http://www.axis.com/products/cam_207/

Descargado el 5-SEP-08

18. Honeywell Security & Communications. LYNXR Alarm Panel.

http://www.security.honeywell.com/hsc/products/control/wi/ly/14964.html

Descargado el 5-SEP-08

CURRÍCULOS

Juan David Osorio Betancur. Ingeniero Telemático de la Universidad Icesi, profesor e investigador de la misma Universidad, vinculado al grupo i2T. Ha realizado investigación en el área de desarrollo de aplicaciones móviles, planeación de redes inalámbricas y computación en malla aplicada a problemas de finanzas y economía.

Luis Ernesto Cárdenas. Ingeniero Electrónico de la Universidad del Valle. Tiene experiencia en técnicas de inteligencia computacional, procesamiento digital de señales y de imágenes, desarrollo de aplicaciones visuales, programación de microcontroladores, interfaces e instrumentación. Actualmente se desempeña como gerente general de Genia Tecnología, profesor hora cátedra de la Universidad Icesi e investigador vinculado al grupo i2T de la misma Universidad.

Rodrigo Bedoya. Ha cursado estudios en Ingeniería Eléctrica y Electrónica en la Universidad Autónoma. Tiene amplia experiencia en administración y monitorización de seguridad en redes, montajes e implementaciones de defensa en profundidad, y experiencia en hacking ético. Trabaja actualmente en Sistemas TGR, S.A.

Cristian Latorre. Estudiante de Física de la Universidad del Valle, y desarrollador de software en Sistemas TGR S.A. Sus áreas de interés son: Instrumentación Electrónica, Seguridad Informática, Plataformas UNIX / POSIX.

Juan Manuel Madrid Molina. Ingeniero de Sistemas y Especialista en Gerencia de Informática de la Universidad Icesi. Cursó estudios doctorales en Ciencias de la Computación en la Universidad de Kansas. Actualmente ejerce como profesor investigador de tiempo completo y director del programa de Ingeniería Telemática de la Universidad Icesi. Sus áreas de interés son la seguridad informática, y la planeación y gestión de sistemas informáticos.