INGENIERÍA DE SEGURIDAD US
E.T.S. Ingeniería Informática. Universidad de Sevilla
Avda. Reina Mercedes s/n. 41012 Sevilla
Tlf/Fax 954 557 139 **E-mail** lsi@lsi.us.es **Web** www.lsi.us.es

PAI 1. SISTEMA DE DETECCIÓN DE INTRUSOS (HIDS) PARA ALMACENAMIENTO MASIVO BASADO EN VERIFICADORES DE INTEGRIDAD

Introducción

Host Intrusion Detection Systems (HIDS) consiste generalmente en software instalado en un sistema informático local. Son muy similares a los sistemas de protección de virus. HIDS representa un método configurable y preciso para la detección de intrusiones, pero es más intensivo administrativamente que los ***Network Intrusion Deteccion Systems*** (NIDS) y, en una empresa con varios servidores, podrían ser substancialmente más costosos. Este software podría utilizar las técnicas que incorporan las API de los diferentes lenguajes de programación para comprobar la integridad de los datos (véase ficheros de los sistemas, configuraciones, etc.) a lo largo del tiempo mediante la generación de resúmenes (message digests o checksums). También se pueden usar herramientas comerciales y de software libre e incluso ciertas funcionalidades de los sistemas operativos por medio de scripts.

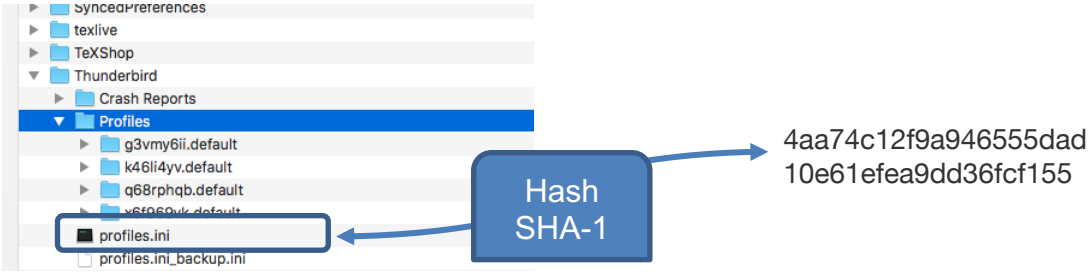


Figura 1: Cáculo de un hash SHA-1

Todo esto se agrava cuando tenemos sistemas de almacenamiento masivo en la nube donde tenemos miles/millones de ficheros con datos almacenados y hacer la gestión de la integridad requiere de medios más sofisticados como la generación de estructura de datos o algoritmos específicos o mecanismos para determinar la integridad sin realizar la descarga de los archivos. Por lo tanto, necesitamos mecanismos eficientes para verificar la integridad.

Figura 2: Problemática de Integridad en los sistemas de almacenamiento masivo.

Necesitamos dotar al HIDS de estructuras de datos y/o algoritmos que mejoren la eficiencia a

la hora de localizar y verificar su integridad. En la Figura 3 tenemos el flujo de un sistema HIDS donde se pide el acceso a un fichero y el HIDS hacer la comprobación de verificación de integridad devolviendo al usuario si el fichero está integro o no. Si el fichero no está integro quiere decir que la información almacenada por el HIDS el momento de realizar la comprobación de la integridad no coincide con la información que el usuario a mandado al servidor para comprobarlo, por lo tanto, existe una inconsistencia y debemos actuar trazar (en un log) dicha inconsistencia en el sistema.

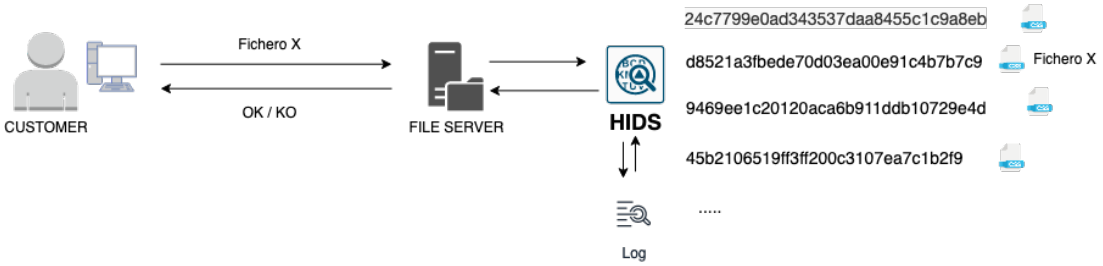


Figura 3: Funcionamiento de HIDS en sistema de almacenamiento tipo nube..

Política y Controles de Seguridad

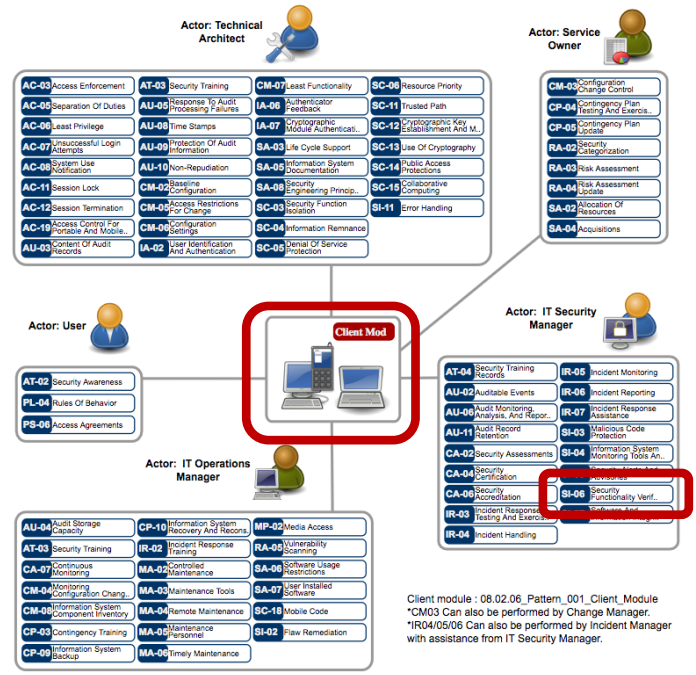
En este **Proyecto de Aseguramiento de la Información** (PAI) se pretende comenzar a familiarizarse con del trabajo en el **gobierno/gestión/tecnologías de la seguridad de la información** y en este caso de la verificación de la integridad de datos/información en un sistema informático de almacenamiento masivo simulado en un host local. Por ello en este PAI se tiene **que dentro de una organización** se ha definido una **Política de Seguridad**, que indica:

*"Debe verificarse **diariamente** la integridad de los **ficheros binarios, de imágenes y directorios de los sistemas informáticos críticos y las aplicaciones de la organización** y **dar cuenta mensualmente** al ISG de la organización de los resultados diarios de la verificación"*

Esta política está bien soportada por la ***Open Security Architecture (OSA)*** donde se definen diferentes módulos, como, por ejemplo, el de cliente (***SP001-Client Module***) o de servidor (***SP-002: Server Module)*** que nos proporciona una perspectiva completa de los diferentes controles a desplegar desde diferentes puntos de vista/roles. Para cada uno de los módulos podemos encontrar una pequeña descripción, como ejemplo la descripción a continuación del módulo de cliente:

***"Description:** Generic end user client module showing appropriate controls that should be applied to all desktop, laptop or mobile clients that process information or access other information systems."*

Acompañado a dichos módulos se puede observar una descripción gráfica de los diferentes controles según el perfil de aplicación como por ejemplo la figura que está a continuación se muestra los controles específicos para un cliente.



Podemos destacar y resaltado en la imagen, desde la perspectiva de un actor de ***IT Security Manager*** se establece el control ***SI-07 Software And Information Integrity,*** que indica:

*"**Control:** The information system detects and protects against unauthorized changes to software and information."*

Este control da respuesta y soporte a la política indicada por tanto la **Dirección** de la organización solicita ayuda al **Equipo de TI de INSEGUS** para el desarrollo/despliegue de una aplicación y realizando la correspondiente gestión de ésta. Dicha aplicación deberá llevar a cabo la **verificación de integridad especificada en la Política de la forma más eficaz y eficiente posible.**

Recomendación de la Dirección – Equipo TI

La Dirección de la organización mediante reuniones con el Equipo de TI de INSEGUS han definido un protocolo de verificación de integridad basado en el diagrama que se muestra en la Figura 4.

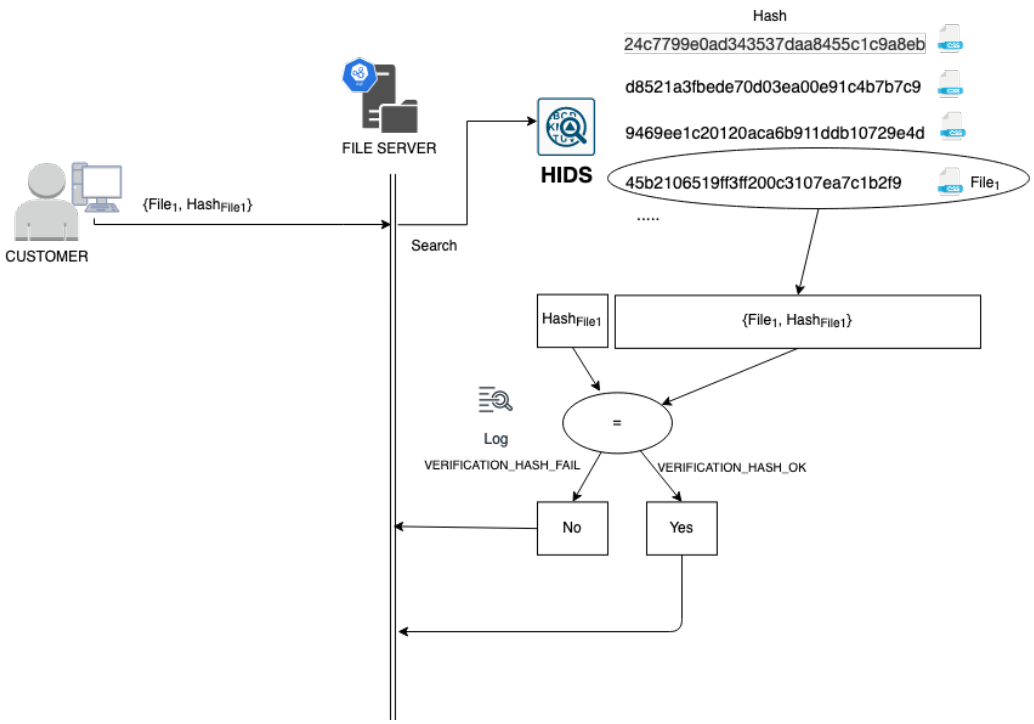


Figura 4: Protocolo de verificación de integridad

Para detallar el funcionamiento interno del sistema HIDS se ha realizado un modelado de procesos que describe el proceso interno de este como se observa en la Figura 5.

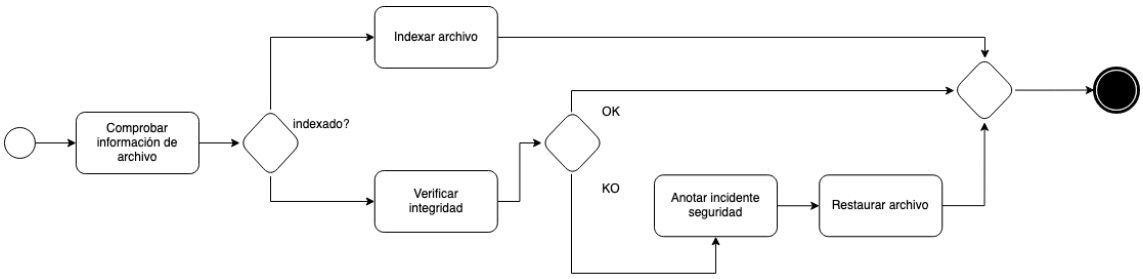


Figura 5: Proceso de comprobación de.

Objetivos del proyecto

A continuación, se propone a los equipos de trabajo los siguientes objetivos:

1. Desarrollar/Seleccionar el más conveniente HIDS basado en verificadores de integridad de acuerdo con lo exigido en la *Política de Seguridad*.
2. Desplegar el HIDS en un sistema de información simulando con cientos/miles de ficheros de diferente tipo.
3. El proceso de verificación se realizará a intervalos, en este caso diariamente y debe almacenarse un informe de un mes entero.
4. Se deberá evitar en mayor o menor medida las debilidades típicas de los HIDS.
5. Se debe razonar y demostrar la eficiencia de la solución aportada a la hora de localizar, calcular y almacenar del HIDS.

Normas del entregable

- Cada Security Team debe entregar a través de la Plataforma de Enseñanza Virtual y en la **actividad** preparada para ello un archivo zip, nombrado ***PAI1-STXTrabajoY*.zip**, que deberá contener al menos los ficheros siguientes:
  - ✓ **Documento en formato PDF que contenga un informe/resumen del proyecto** con los detalles más importantes de las decisiones, soluciones adoptadas y/o implementaciones desarrolladas, así como el resultado y análisis de las pruebas realizadas (máximo 10 páginas).
  - ✓ **Código fuente de las posibles implementaciones o scripts desarrollados o configuraciones establecidas en herramientas ya disponibles.**
- El plazo de entrega de dicho proyecto finaliza el **día 1 de marzo a las 12:30 horas.**
- Los proyectos entregados fuera del plazo establecidos serán considerados inadecuados por el cliente y por tanto entrarán en penalización por cada día de retraso entrega de 5% del total, hasta agotarse los puntos.
- **El cliente no se aceptará envíos realizados por email, ni mensajes internos de la enseñanza virtual, ni correo interno de la enseñanza virtual. Toda entrega realizada por estos medios conllevará una penalización en la entrega del 5%.**

Métricas de valoración

Para facilitar el desarrollo de los equipos de trabajo el cliente ha decidido listar las métricas que se tendrán en cuenta para valorar los entregables de cada grupo de trabajo:

- **Documento (30%)**
  - Tamaño del informe
  - Calidad del informe aportado y justificaciones.
  - Calidad de pruebas presentadas y resultados
- **Código/Configuración aportada (70%)**
  - Cumplimiento de requisitos establecidos
  - Calidad del código entregado
  - Complejidad de la automatización
  - Recolección de métricas y reportes
  - Pruebas entregadas