Departamento de Lenguajes y Sistemas Informáticos
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

E.T.S. ingeniería informática

SEGURIDAD EN SISTEMAS INFORMÁTICOS Y EN INTERNET

PAI 1. SISTEMA DE DETECCIÓN DE INTRUSOS PARA HOST (HIDS) 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.

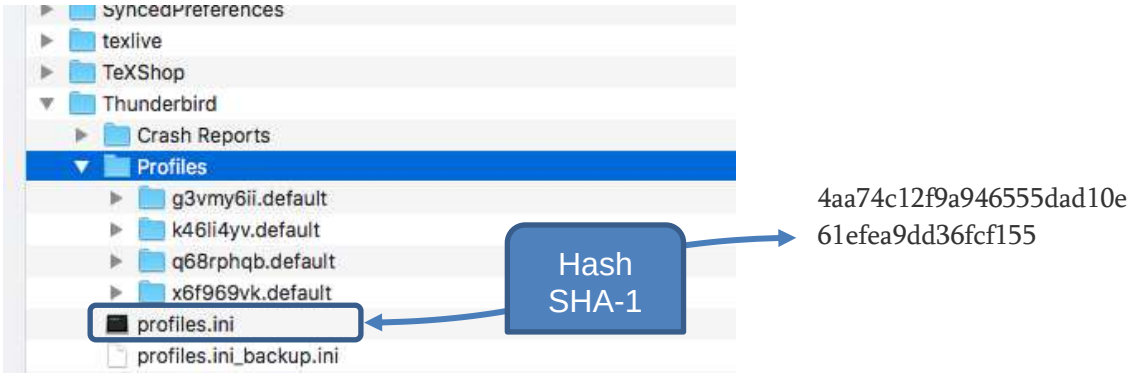


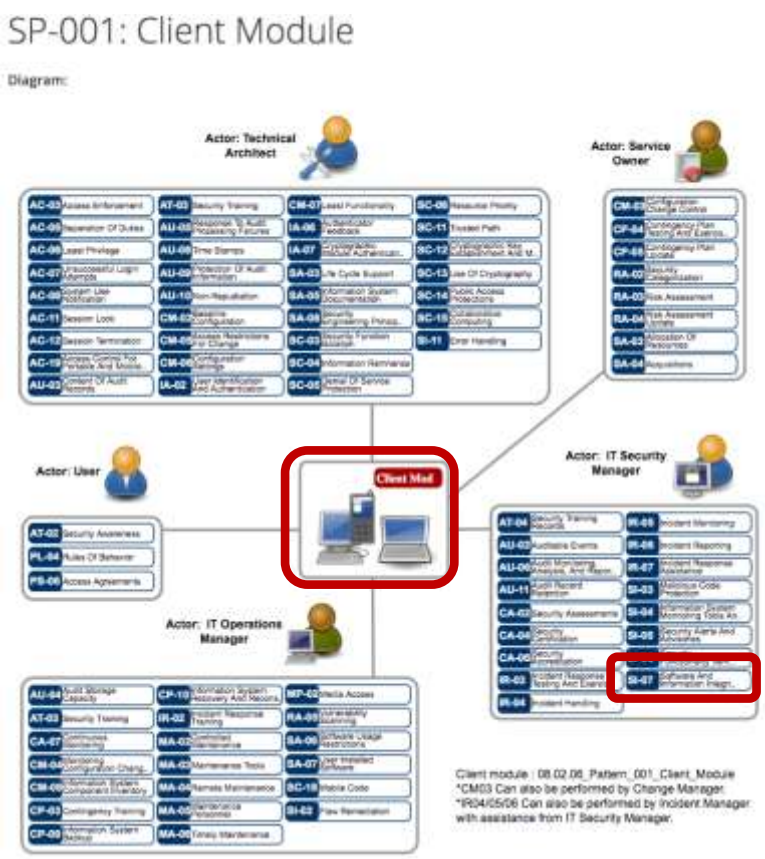
Figura 1: Cáculo de un hash SHA-1

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. **Dentro de la organización** se ha definido una **Política de Seguridad** que indica:

*"Debe verificarse **diariamente** la integridad de los **ficheros binarios/directorios de los sistemas informáticos críticos y las aplicaciones/páginas Web 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 define el módulo de cliente ***SP001-Client Module***:

*"**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."*



Desde la perspectiva de un actor de IT Security Manager como el que van a desarrollar los equipos de trabajo se establece el control ***SI-07 Software And Information Integrity*** que establece:

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

La **Dirección** solicita ayuda al **Equipo de TI** mediante el desarrollo/despliegue de una aplicación y realizando la correspondiente gestión de esta. Todo ello llevará a cabo la **verificación de integridad especificada en la Política de la forma más eficaz y eficiente posible.**

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 informático con más de mil ficheros (lo más heterogéneos posibles).**
3. **La verificación se realizará a intervalos, en este caso mínimo cada 60 minutos, y debe almacenarse para generar un informe con periodicidad (por ejemplo, de un día entero).**

4. **Establecer un sistema de alerta, y de monitorización de la Política mediante algún indicador. Por ejemplo, se puede usar la evolución de la ratio (porcentaje %) de ficheros no corruptos con respecto a los analizados, si baja del 100% y sigue decreciendo podemos estar ante un ataque.**
5. **La solución propuesta deberá evitar en mayor o menor medida las debilidades típicas de los HIDS**
6. Se deben realizar las correspondientes pruebas para comprobar el correcto funcionamiento de lo desplegado/desarrollado y presentar un resumen de las pruebas realizadas en el informe final del trabajo.

Factores y debilidades que se deben tener en cuenta a la hora de seleccionar la implementación más adecuada del HIDS

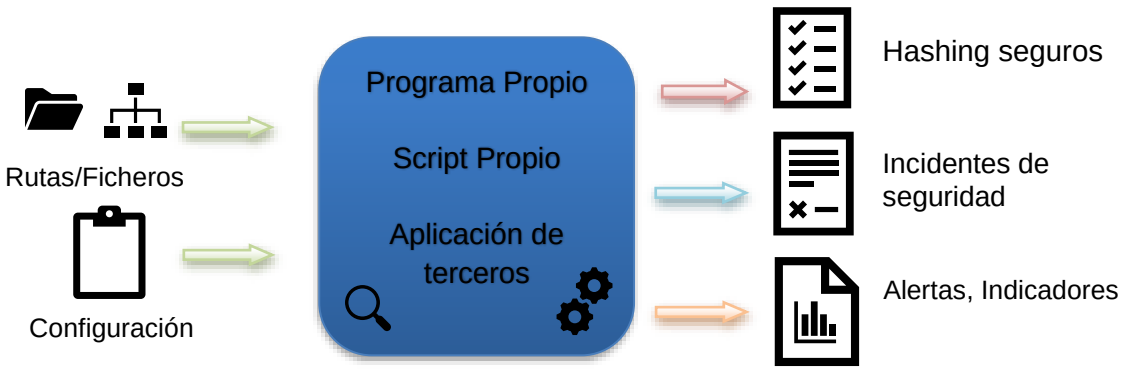
HIDS tienen muchos puntos débiles que pueden explotarse por un atacante o producir frecuentes alertas por falsos positivos. Se deben analizar en la propuesta las debilidades de los HIDS, y tratar de evitarlas en la propuesta:

1. ¿Hay colisiones frecuentes de los hashing seguros elegidos?
2. El atacante podría acceder al fichero que guarda los hashing seguros, ¿se encuentra protegido para evitar/dificultar su posible modificación?, ¿está ubicado en una zona segura?
3. ¿Puede un atacante eliminar el verificador de integridad o simplemente recalcular los hashing y cambiar el fichero original?
4. ¿Las alarmas que se generan son demasiado tardías para su uso?, ¿el atacante puede llegar a deshabilitar el HIDS antes de darnos cuenta del ataque?

Propuesto de la Dirección - Recomendaciones

Para llevar a cabo los objetivos del proyecto nos solicitan que el proyecto siga las siguientes recomendaciones:

- **Configuración:** debe permitir seleccionar un conjunto de carpetas/ficheros en los que se deba verificar la integridad. Se debe poder establecer el intervalo de tiempo donde se realizará la comprobación de la integridad. Se valorará la posibilidad de elegir entre diferentes algoritmos para verificar la integridad.
- **Acceso a las incidencias y presentación de resultados:** se debe tener acceso a las incidencias de seguridad relacionadas con la integridad. Se debe al menos tener acceso a la información de los ficheros que no han conservado la integridad, señalando la hora y día en la que se hicieron las verificaciones.



Normas del entregable

- Cada grupo debe entregar a través de la Plataforma de Enseñanza Virtual y en la **actividad** preparada para ello un archivo zip, nombrado ***PAI1-GrupoX*.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 15 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 2 de noviembre a las 8:30 horas.**
- Los proyectos entregados fuera del plazo establecido serán considerados inadecuados por el cliente y por tanto entrarán en penalización por cada día de retraso entrega de 10% 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 10%.**

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%)**
  - Calidad del informe aportado y justificaciones
- **Código/Configuración aportada (70%)**
  - Cumplimiento de requisitos establecidos
  - Calidad del proyecto entregado
  - Complejidad de la automatización
  - Calidad de pruebas presentadas y resultados