ACUO: Aplicación de Control de Usuarios y Ordenadores

ACUO: Users and Computers Control Application

J. A. Lorenzo, J. C. López, P. Cerdán et al.

Esta herramienta denominada ACUO permite conocer la utilización de las aulas informáticas y poder limitar el uso de programas no permitidos

Resumen

Vamos a describir una herramienta para conocer y controlar el uso que se hace de los ordenadores.

Esta herramienta denominada ACUO (Aplicación para el Control de Usuarios y Ordenadores) permite conocer la utilización de las aulas informáticas y poder limitar el uso de programas no permitidos. Nos planteamos utilizar un antivirus como un "antijuegos". Ante la imposibilidad de incluir nuestras propias firmas "antijuegos" en un antivirus comercial hemos creado nuestra propia herramienta.

ACUO es una aplicación basada en un agente capaz de saber qué, cuándo, quién y dónde se ejecuta en cada ordenador bajo control. En base a esta información podemos llevar a cabo desde una explotación estadística de los datos, hasta un control que únicamente permita el funcionamiento de una lista limitada de programas. La aplicación nos proporciona un conocimiento del uso de las aulas que nos permite planificar y gestionar los recursos en base a los datos que proporciona.

Veremos cómo a partir de los registros hemos obtenido los patrones de utilización del hardware y el software objeto del análisis que presentamos en forma de gráficas.

Palabras clave: Control, usuarios, agente, estadísticas, utilización

Summary

The so called ACUO is a tool to know and control the usage of computers. It allows the knowledge of classrooms and laboratories computer utilization, and limits the use of not allowed programs. It's like using a virus scanning program as a game scanning program. Facing the impossibility to add our own anti games signs in a commercial virus scanning program, we have created our own tool.

ACUO is an application able to know where, when, what and who is executing in each computer under control. Having this information we can make a range of statistics and a list of banned programs. Based on the data provided, we can knowl about use in classrooms, and assist in managing and planning of resources.

From registers and logs we get hardware and software utilization patterns involved and these wil be shown in a graphic form.

Keywords: Control, users, agent, statistics, utilization

1.- Introducción y marco tecnológico

La herramienta que hemos desarrollado nos da solución a la situación de falta de datos y de control del uso de los ordenadores en las aulas informáticas. Nos encontramos en un entorno de estudios de ingeniería donde los alumnos han de disponer de espacios con la máxima flexibilidad posible para poder desarrollar sus prácticas docentes, pero a la vez no podemos perder el control ni permitir un mal uso de la red y los recursos informáticos. Nuestros alumnos disponen de un usuario personal y único para entrar a las aulas y pueden trabajar sobre dos sistemas operativos distintos: Windows 2000 professional y Linux.

2.- Objetivo

Nuestra intención al desarrollar esta aplicación es poder disponer de datos objetivos sobre la utilización de los recursos informáticos y así ser capaces de controlar un posible mal uso. Además nos propusimos hacer un entorno centralizado desde donde controlar todos los eventos.

3.- Desarrollo e implantación

3.1.- Componentes básicos

a) Generales:

- Un fichero de firmas que contiene por cada programa que hayamos añadido la firma MD5 calculada por franjas y la clasificación de dicho programa.

- Una herramienta para clasificar programas como:

  - Prohibidos: Se impide su ejecución.
  - Controlados: Se registra el inicio y el final de su ejecución.
  - De inicio de sesión: Clasificamos así un programa que se ejecuta cada vez que un usuario entra en la máquina.

b) Para el control en Windows:

- Una librería DLL para Windows que será llamada cuando se ejecuten los programas.
- Una DLL de control para Windows, con funciones de generación de firma, determinación del tipo de programa y actuación por cada tipo que tenemos.

c) Para el control en Linux:

- Dos módulos PAM para autentificar usuarios y montar volúmenes Netware.

d) Para el cálculo estadístico:

- Una serie de clases Java de análisis de logs y generación de gráficas.

3.2.- Control en Windows

Para efectuar el control de aplicaciones en este sistema operativo, instalamos en cada cliente una pequeña DLL y modificamos el registro de tal forma que hacemos que esta librería se añada en el inicio de ejecución al espacio de direcciones de cualquier programa Windows que utilice la librería USER32.DLL.

Cuando un programa de estas características se ejecuta, nuestra DLL se carga. En ese momento llama a otra DLL de control que tenemos en red. En caso de que el acceso fallase, cargarí una copia local.

La librería de control genera la firma MD5 por franjas del programa ejecutado y la compara con las del fichero de firmas que hay en la red. Si no se puede acceder a dicho fichero, se utiliza una copia local del mismo.

Una vez que nuestra librería de control determina el tipo de programa, actúa de la siguiente manera:

- Si es un programa que hemos calificado como prohibido, finaliza su ejecución.
- Si es un programa calificado como controlado registra un evento de inicio de ejecución y lanza otro proceso que esperará a que finalice el programa para registrar el evento de final de ejecución.
- En el caso de un programa que hayamos calificado como de inicio de sesión registra un evento de login de usuario y lanza otro proceso que esperará a que el usuario cierre la sesión para registrar el evento de logout de usuario.

La librería de control genera la firma MD5 por franjas del programa ejecutado y la compara con las del fichero de firmas que hay en la red

Cuando se planteó la necesidad de procesar los registros generados, se tuvieron en cuenta varias plataformas para el desarrollo de las aplicaciones

3.3.- Control en Linux

La autentificación del usuario se realiza contra el NDS de Netware gracias a un módulo PAM (Pluggable Authentication Module) llamado pam_nw_auth. Una vez se ha permitido el acceso, otro módulo, pam_mount, se encarga de montar de manera automática y transparente el volumen Netware en donde se guarda el registro de entradas y salidas. Mediante la ejecución de un script al montar, se registra el login y al desmontar el logout. En el registro de cada evento, se incorpora en cada línea, entre otra información, el nombre de la máquina que se obtiene mediante DNS.

3.4.- Cálculo de estadísticas

3.4.1.- Estadística y explotación de logs

Cuando se planteó la necesidad de procesar los registros generados, se tuvieron en cuenta varias plataformas para el desarrollo de las aplicaciones. Se eligió Java 2 SDK SE por los siguientes motivos: Posibilidad de ejecución de la aplicación mediante un servidor de aplicaciones web, flexibilidad de uso en diferentes sistemas operativos, visualización de resultados en cualquier navegador de Internet mediante applets, y que las herramientas de desarrollo son de libre distribución.

Realizamos estadísticas de utilización de los ordenadores, control de licencias, sistemas operativos usados, y filtros de búsqueda por usuario o por ordenador.

3.4.2.- Utilización y número de usuarios

Los agentes de control de Windows y Linux generan un registro de sesiones. Cada línea del mismo tiene el siguiente formato:

LOGIN | LOGOUT;NOMBRE ORDENADOR;DIA;HORA;SISTEMA OPERATIVO:USUARIO

Con esta información extraemos los datos de utilización. Se ha querido desde un principio que la presentación de los resultados fuera gráfica, vistosa y de fácil interpretación. Además el uso de los ordenadores se realiza, en nuestras aulas y laboratorios, de manera diaria de 08:30 h. a 21:00 h..De este planteamiento inicial se derivan los parámetros de diseño:

- Utilización máxima de ordenadores.
- Presentación del número de usuarios que abren una sesión
- Resolución de 1 hora para determinar los resultados anteriores.
- Filtro por espacios (aulas y laboratorios)
- Filtro por fechas. Dados los días lectivos, 14 periodos de 1 hora por día y el espacio en una hoja DINA4, se han elegido periodos de quince días por gráfico.

La utilización será:

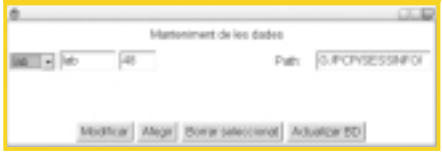
$$\frac{\sum_{PC} \frac{H_{salida} - H_{entrada}}{60}}{N^{o}\ total PC}$$

Para filtrar las líneas del registro por espacios se utilizan los nombres NETBIOS de los ordenadores, que deben coincidir con los IP. Previamente se ha aplicado una política de asignación de nombres dependiendo del sitio donde se hallan estos. Por ejemplo, en el Laboratorio 1 todos los nombres

tienen el prefijo LAB1. También se necesita introducir cuántos ordenadores hay en cada espacio para obtener el tanto por ciento máximo de utilización.

MENÚ DE SELECCIÓN DE PARÁMETROS

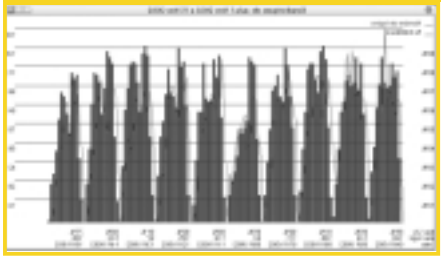
MENÚ DE INTRODUCCIÓN Y MODIFICACIÓN DE PARÁMETROS



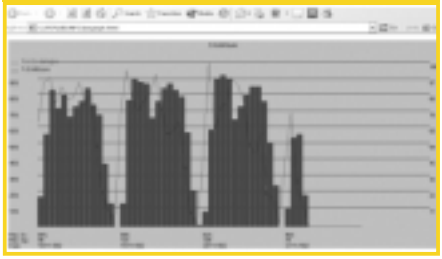
Para la representación gráfica se utiliza una barra para cada hora y tanto por ciento de utilización, y una línea que indica el máximo de sesiones en esa hora. El ancho de las barras es escalable, dependiendo del número de días de la estadística.

Al pie del gráfico se muestra, la máxima utilización y el máximo nímero de usuarios, de todo un día.

UTILIZACIÓN DE LAS AULAS



UTILIZACIÓN DE LAS AULAS DE 3,5 DÍAS VISTA COMO APPLET



3.5.- Control de licencias

La librería de control de programas genera un registro para cada ordenador controlado. Cada línea tiene este formato:

INICIO | FINAL DE EJECUCION: DIA : HORA : RUTA DEL EJECUTABLE CONTROLADO

Con los registros de todos los ordenadores, y los mismos planteamientos de diseño de las gráficas anteriores, definimos los parámetros del gráfico:

- Número de licencias abiertas simultáneamente.
- Resolución de 1 minuto en el cálculo.
- Filtro por fechas. Representación de 15 días.
- Dados los parámetros anteriores, 14 horas diarias de acceso y el espacio en una hoja DINA4, se han elegido puntos de 20 minutos para el gráfico.
- Selección de una aplicación controlada.

La herramienta para clasificar y crear la firma de cada ejecutable, genera un registro con la firma, tipo de aplicación y ruta. De este archivo el menú de selección lee los ejecutables, y los presenta en un desplegable.

La herramienta para clasificar y crear la firma de cada ejecutable, genera un registro con la firma, tipo de aplicación y ruta

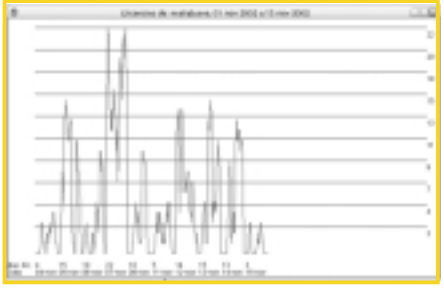
3.6.- Menú de selección de parámetros

Se desprecian las aplicaciones que sólo se hayan utilizado durante 1 minuto. Así pues cada punto de la curva representa, el número máximo de aplicaciones abiertas simultáneamente en 20 minutos, durante más de 1 minuto.

Al pie del gráfico se muestra, el máximo número de licencias utilizadas en 1 día.

LICENCIAS UTILIZADAS EN 1 DÍA

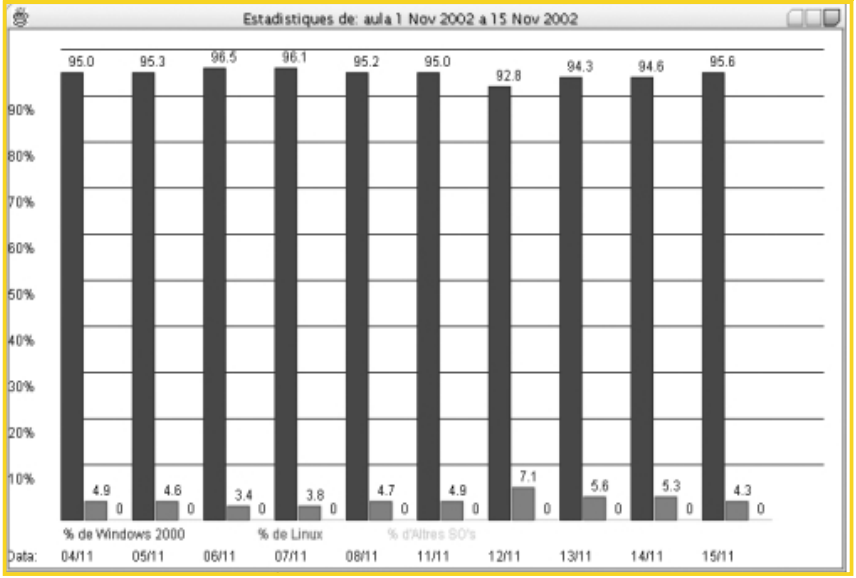
LICENCIAS ABIERTAS DE MATLAB



3.7.- Sistemas operativos

Mediante el mismo registro de sesiones antes descrito y los mismos filtros, por espacio y fechas, que utilizaba el gráfico de utilización, representamos el uso de sistemas operativos.

USO DE SISTEMA OPERATIVO



4.- Ventajas sobre la situación actual

Actualmente podemos saber cómo se utilizan los recursos, con una herramienta flexible y sencilla. Además podemos controlar el mal uso y prohibir la ejecución de programas no permitidos por la normativa del utilización de las aulas informáticas del centro.

Actualmente podemos saber cómo se utilizan los recursos, con una herramienta flexible y sencilla

5.- Conclusiones y líneas de trabajo

Actualmente estamos trabajando en la explotación de datos para poder detectar qué usuario ha estado trabajando en una máquina en un momento concreto, y en la presentación gráfica de los datos; de modo que pueda contrastarse el uso real en los horarios de prácticas con los calendarios de reserva de los espacios para docencia.

José Antonio Lorenzo
(joseantonio.lorenzo@uab.es)
José Carlos Lopez, Pere Cerdan,
Raúl Martos, Olivia López, Mónica Herrera
S.I.E.E.
(siee.etse@uab.es)
Soporte Informático de la ETS de Ingenieria
UAB