UMGina: Sistema de Control de Acceso en Aulas Basado en Tarjetas Inteligentes de la Universidad de Murcia.

Autores:
Fº Javier García Ros, Fº José Hidalgo Céspedes, Mª Soledad Navarro España, Josefa Gil Valera, Oscar Cánovas Reverte, Tomás Jiménez García
[*jgarcia, jhidalgo, marisol ,pepi, ocanovas, tomasji]@fcu.um.es*
Gregorio Martínez Pérez, Antonio Gómez Skarmeta
[*gremar,skarmeta*]*@dif.um.es*

1. RESUMEN

El Servicio de Informática de la *Universidad de Murcia*, ha desarrollado un sistema de control de acceso basado en la utilización de tarjetas inteligentes, para sus equipos en aulas de libre acceso (*ALAs*), complementando así otros elementos de seguridad como son: autenticación, integridad, confidencialidad y no repudio abordados por otros proyectos de la misma Universidad [1, 2] dotando de un sistema global de control y gestión de reservas transparente al usuario y fácil de administrar.

2. ANÁLISIS DEL PROBLEMA

Los sistemas de control de acceso a recursos informáticos, son de enorme interés sobre todo cuando dichos recursos generalmente están limitados y nos encontramos en un entorno con grandes comunidades de usuarios.

Las soluciones actuales ofrecidas por sistemas operativos como Unix o Windows, y que están basadas en la validación de un par *login/pasword*, son insuficientes debido a que plantean diversas deficiencias (se suele trabajar con perfiles por puesto, y no por persona). En las ALAs de la Universidad de Murcia, se venía utilizando un esquema basado en un login genérico por puesto debido a la dificultad de tener una cuenta para cada uno de las decenas de miles de usuarios. Esta razón imposibilitaba tener un control sobre la identidad y duración de la sesión, ya que en el momento en el que el usuario entra en el sistema, no existían mecanismos sencillos y económicos para poder controlar, de esta forma, cuestiones como el tiempo que tiene disponible el usuario.

Tampoco nos permite una gestión centralizada de los recursos, que dé pie a racionalizar su utilización por parte de una comunidad de usuarios, a través de, por ejemplo, una política de control de accesos y un sistema de reservas previas.

3. ENTORNO

La Universidad de Murcia gestiona en la actualidad, a través de su Servicio de Informática, un total de 21 ALAS. Dichas aulas están equipadas con ordenadores PC con sistema operativo **Microsoft Windows NT 4 Workstation** conectados todos ellos a la Intranet de la Universidad de Murcia y con acceso a Internet. Dentro de sus características hardware cabe destacar la utilización **lectores de tarjetas inteligentes**.

Actualmente las reservas de puestos en ALAS se hacen a través de las **secretarías virtuales** de la Universidad de Murcia, donde el usuario puede seleccionar el día, hora y lugar de un puesto de trabajo.

4. OBJETIVOS

Los objetivos que nos planteamos a la hora de desarrollar UMGina fueron los siguientes:

- Evitar el uso indebido de puestos amparándose en el anonimato.
- Realizar un control de reservas sin necesidad de personal dedicado.
- Bloqueo sistemático de puestos no reservados y usados.
- Cumplimiento de los tiempos de reserva.
- Cumplimiento de la política de control de acceso.
- Control estadístico del uso de puestos.

5. REQUISITOS DEL SISTEMA

Como cualquier sistema de control de acceso, el sistema debe ser **difícil de quebrantar** y aún en ese caso, que su detección sea posible.

El medio de autenticación será la **tarjeta inteligente** de la Universidad de Murcia que poseen todos sus usuarios (estudiantes, personal de administración y servicios y personal docente e investigador).

Que el sistema sea **sencillo de instalar y administrar**.

6. SOLUCION

UMGina es la solución software que se encuentra en los ordenadores clientes, capaz de gestionar todos los eventos relacionados con la sesión de un usuario. Para conseguir este objetivo hemos modificado el sistema de control de accesos de Microsoft Windows NT 4 [3], por un módulo propio conocido como *UMGina* (*University of Murcia Graphical Identification aNd Authentication)*. En dicha implementación, se enlaza la gestión de la acción a realizar por parte del propio sistema operativo: abrir, bloquear o cerrar una sesión de usuario, con las operaciones propias sobre la tarjeta inteligente [4]: inserción, extracción, validación del PIN, lectura de datos administrativos, etc., y el sistema gestor de acceso y reservas. Tras su instalación, procede a tomar el control del módulo de accesos de Windows NT, reemplazando el esquema tradicional de *login/password*, por otro basado en la utilización de la tarjeta inteligente de la Universidad de Murcia.

Este módulo junto al subsistema de gestión de reservas y la política de acceso forman la base del sistema de Control de Acceso en Aulas de la Universidad de Murcia.

7. MODO DE OPERACION

Cuando un usuario desea reservar un ordenador, accede haciendo uso de su tarjeta inteligente, al sistema de reservas instalado en las secretaría virtuales, que le informa de la disponibilidad de los equipos en las distintas ALAs, a partir de los datos almacenados en la BD de reservas; una vez hecha la selección deseada (de aula, día y hora), el sistema notifica al usuario, el puesto sobre el cual tiene hecha la reserva.

Llegado el momento, y con la finalidad de hacer uso de la reserva, el usuario debe de introducir su tarjeta inteligente en el lector del equipo sobre el que tiene la reserva; este evento de

inserción es detectado por el módulo *UMGina* que procede a autenticar al portador de la tarjeta, pidiéndole su *PIN*; si la validación es correcta, la tarjeta no está caducada y pertenece a la Universidad de Murcia, dicho módulo lee los datos de identificación de la persona, y del equipo al cual se pretende acceder, y establece una comunicación segura [6, 7] con el sistema de reservas; este sistema informa sobre la existencia (o no) de una reserva que cumpla los parámetros indicados, y en función de la respuesta y de lo indicado en la política de control de accesos de la Universidad, UMGina procede a abrir (o no) la sesión de trabajo. Si la operación se desarrolló con éxito, en la base de datos de reservas queda constancia de este evento dandonos la bienvenida en pantalla con su nombre e incluso siendo posible mostrar su fotografía. El sistema también nos indica si el usuario ha sido sancionado por alguna razón y no puede hacer uso de la reserva, o si en ese momento el puesto está reservado por otra persona, ya que el sistema le da un margen de tiempo para poder hacer uso de ésta; pasado ese tiempo, otra persona puede solicitar entrar en el puesto, dejando constancia en la base de datos.

El usuario podrá hacer uso del puesto durante el periodo de tiempo que se le haya indicado en el inicio de sesión. Según se va acercando esta cota temporal, UMGina realiza sucesivas notificaciones por consola, indicando la conveniencia de almacenar el trabajo realizado e ir finalizando la sesión. Una vez cumplido el tiempo de sesión el sistema preguntará si se desea ampliar el tiempo de reserva. Si no hay una reserva posterior sobre ese ordenador, el sistema ampliará nuestro tiempo de sesión; si, por el contrario, la reserva posterior existe, procede a cerrar la sesión permitiendo que la siguiente persona pueda hacer uso de su reserva.

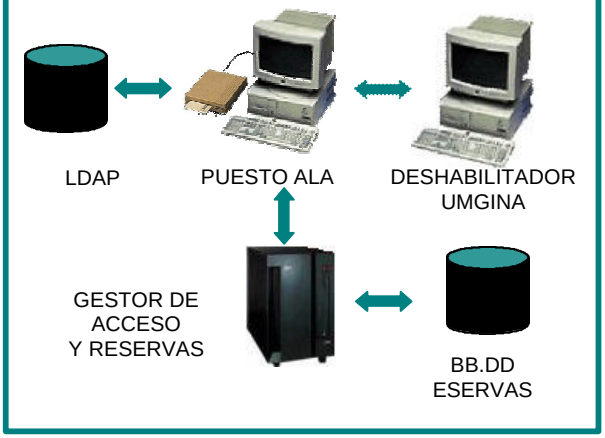
Según se ha definido en la política de control de accesos, se obliga a que el usuario tenga introducida su tarjeta durante el tiempo que se encuentra en el ordenador. Si el usuario decide extraer su tarjeta del lector, su sesión quedará bloqueada automáticamente hasta que la vuelva a introducir, en cuyo caso su sesión seguirá en el mismo estado en el que la dejó. Si el tiempo de sesión termina y el puesto sigue bloqueado, se procederá a la finalización de la sesión, perdiendo en su caso, el trabajo no almacenado. Un administrador también podría forzar la finalización de la sesión con las mismas consecuencias que el caso anterior.

Cuando el usuario decide terminar con su sesión, simplemente indica su salida al sistema, el cual se encarga de realizar un apunte en la base de datos sobre el fin de la sesión; si a partir de éste momento, hubiera suficiente tiempo hasta la próxima reserva, cualquiera podría utilizar el ordenador, sin necesidad de haber formalizado una reserva previamente, y quedando registrado esta entrada en la base de datos sin más que introducir su tarjeta.

Hay determinadas personas que deben tener posibilidades de entrar como administradores al puesto. Cuando UMGina detecta la inserción de estas tarjetas y después de validado su PIN, muestra un cuadro de dialogo típico de Windows NT para que introduzca el usuario con que quiere entrar, el password y el dominio. Si UMGina detecta la intrusión como usuario *administrador* sin tener esta tarjeta este perfil, queda constancia del evento y no permite la entrada.

Si por alguna razón la base de datos no estar operativa, el administrador de las ALAS, puede desactivar el uso del gestor de acceso y reservas trabajando de forma local y almacenando en ficheros locales la identidad, horas de entrada y salida, etc. , hasta que la base de datos se recupere, mandando estos registros posteriormente a la base de datos, para poder hacer consultas en línea. En la figura 1 podemos observar un esquema de la arquitectura del sistema.

Figura 1: Arquitectura de UMGina



8. CONCLUSIONES Y TRABAJOS FUTUROS

Con la puesta en marcha de este proyecto, la Universidad ofrece máximo acceso a sus usuarios a recursos informáticos, pero a la vez implanta mecanismos de control para protegerse contra el posible mal uso de los mismos. Conseguimos por lo tanto un sistema versátil y económico por cuanto reduce la cantidad de personal dedicado a inspección en cada instalación.

Su arquitectura flexible, nos permite implementarlo en otros sistemas operativos así como adaptarlo a otras instituciones que requieran soluciones de control de acceso, consiguiendo reemplazar el mecanismo clásico de login y password por un medio de amplio valor añadido como es la tarjeta inteligente.

9. BIBLIOGRAFÍA

[1] A.Gómez, J.García, J.Gil, E. Martínez,G. Martínez, A. Caja, O. Cánovas, Experiencia piloto de certificación en la Universidad de Murcia. Noviembre 1998. Disponible en: http://www.rediris.es/rediris/boletin/46-47/ponencia7.html

[2] A.Gómez, J.García, J.Gil, E. Martínez, G. Martínez, A. Caja, O. Cánovas, Providing security to university environment communications. Junio 1999. Disponible en: http://www.terena.nl/tnnc/8A/8A3/8A3.html

[3] Microsoft Corp. Winlogon User Interface. Microsoft Network Developer Library.

[4] PC/SC WorkGroup, Interoperability Specification for ICCs and Personal Computer System, Diciembre 1997. Disponible en: http://www.smartcardsys.com/

[5] M. Wahl, T.Howes, S. Kille. Lightweight Directory Access Protocl (v 3), Request For Comments 2251, 1997.

[6] Alan, Freier, Kocher, The SSL Protocol Version 3.0, Internet Draft, 1996.

[7] Dierks, C. Allen, The TLS Protocol Version 1.0, Request For Comments 2246, Enero 1999.