SIGEBAJA:
GENERACION Y EVALUACIÓN AUTOMATICA DE EXAMENES UN SISTEMA CON AUTENTIFICACIÓN , PRIVACIDAD E INTEGRIDAD.

Luis Martinez
martin@ujaen.es

Francisco Mata
fmata@ujaen.es

Pedro J.Sanchez
Pedroj@ujaen.es

Departamento de Informática
Universidad de Jáen,23070-Jaén, España

Resumen

La incorporación de las Tecnologías de la Información y de la Comunicación al área de la enseñanza, ha producido la aparición de nuevas herramientas que facilitan las distintas tareas que deben llevar a cabo tanto los docentes como los alumnos. En este trabajo nos centraremos en un sistema generador y evaluador de exámenes tipo test denominado SIGEBAJA. Este sistema fue concebido para implantarse sobre una Intranet en un centro educativo, pero debido a su versatilidad puede utilizarse en Extranets e incluso a través de Internet para aumentar las posibilidades de uso. Este sistema genera exámenes tipo test con múltiples respuestas a partir de una Base de Datos de preguntas mediante applets Java. Una vez que hayamos visto el funcionamiento del sistema en una Intranet y sus posibles mejoras para utilizarlo de forma remota mediante una Extanet o Internet, nos centraremos en solucionar un problema fundamental que aparece al trabajar con sistemas que intercambian información a través de líneas de comunicación como es la seguridad. Veremos como dotar a SIGEBAJA de capacidades de Autentificación, Privacidad e Integridad que son los aspectos básicos de seguridad que debe cumplir un sistema que usa líneas de comunicación para considerarse seguro

Palabras clave: Sistema automático, Intranet, Internet, Seguridad, Java..

1. Introducción

En la recta final del siglo XX la sociedad ha experimentado un profundo cambio debido al espectacular avance que han sufrido las Tecnologías de la Información y Comunicación (TIC) hasta el punto que podemos decir que vivimos en la *"Era de la Informática y las Telecomunicaciones"*, que son las áreas tecnológicas o tecnologías que componen las TIC. Dicho avance ha supuesto tal y como indica Coombs [4] una transformación en todos los aspectos de nuestra vida cotidiana como la economía, procesos productivos, ocio, empleo, el entorno educativo, etc. El avance que mayor impacto ha causado en la sociedad en el último lustro ha sido el producido por el desarrollo e implantación de Internet [3] como elemento de uso cotidiano por un número cada vez mayor de usuarios en todo el mundo (oscilando dicho número en cientos de millones).
Una de las áreas en las que se ha producido transformaciones de gran importancia en sus procesos debido a los avances de estas tecnologías es la *"Educación"*. En este trabajo haremos un repaso de las distintas aplicaciones de las TIC en el entorno educativo y nos centraremos en la descripción de un sistema generador y autoevaluador de exámenes tipo test de múltiples respuestas [10]. Dicho sistema será implantado sobre una Intranet en un centro educativo y con la posibilidad de ser utilizado de forma remota fuera de dicho centro a través de una Extranet o de Internet.

Una vez introducido dicho sistema veremos que pueden aparecer una serie de problemas de seguridad a la hora de utilizar el sistema de forma remota, como son problemas de **Autentificación, Privacidad e**

Integridad. [8] [12] Por lo que presentaremos distintas técnicas para solventar dichos problemas de seguridad.
Este trabajo se estructura de acuerdo al siguiente esquema: en la sección 2 repasaremos distintas aplicaciones de las TIC a la enseñanza; en la sección 3 veremos el funcionamiento del sistema SIGEBAJA; en la sección 4 estudiamos los problemas de seguridad del sistema y como solucionarlos y por último presentaremos distintas conclusiones y señalaremos trabajos futuros.

2. APLICACIÓN DE LAS TIC EN LA EDUCACIÓN.

La utilización de las TIC en la enseñanza ha supuesto un importante avance en las metodologías de la educación ya que ha permitido el uso de herramientas como el vídeo, el vídeo interactivo, el ordenador, el CD-ROM, etc..., [9] que hacen más fácil y menos rígido el proceso educativo. De éstas herramientas quizás la de mayor importancia sea el ordenador debido a su capacidad de integrar los anteriores elementos dentro de su utilización, lo que ha dado lugar a metodologías de enseñanza asistidas por ordenador:

- **C.A.L.** (Computer Aided Learning), es decir, el aprendizaje asistido por ordenador
- **C.A.I.** (Computer Aided Instruction), o en español, la enseñanza o instrucción asistida por ordenador.

Estas metodologías emplean el ordenador usando su potencia multimedia que consiste en la integración de información texto, imágenes, sonido y animación [5], lo cual proporciona una enorme capacidad de comunicar de forma clara y sencilla información.

Hasta hace muy poco tiempo la tecnología utilizada para trabajar con información multimedia era el CD-ROM, que es un dispositivo óptico de almacenamiento muy fiable, pero con muchas limitaciones de capacidad y rigidez de su contenido. Estos problemas junto con el desarrollo de las redes de comunicaciones y el abaratamiento de éstas, ha producido un cambio en el modo de acceder a la información Multimedia a través de los ordenadores, ya que al crearse tecnologías que permiten el almacenamiento y transmisión de este tipo de información a través de redes de ordenadores de una forma sencilla y barata (Internet junto con sus protocolos), aportando una serie de valores añadidos que no tiene el CD-ROM como espacio prácticamente ilimitado, dinamicidad de los datos, acceso remoto a la información, etc. Es compresible por tanto, que se esté produciendo un profundo cambio de las tecnologías usadas en la C.A.L. y C.A.I. debido a estas tecnologías.

3. SIGEBAJA: Sistema Generador de Exámenes Basado en Applets Java.

Aquí vamos a hacer una breve descripción del SIGEBAJA (Sistema generador de exámenes basado en applets Java) presentado en [10]. Este sistema se implantará sobre una Intranet con varios puestos cliente y un único puesto servidor.

Definición 1 [5],[2]. *Una Intranet es una red de área local que comunica múltiples usuarios usando la tecnología de Internet. Estas redes ponen un límite al área de acceso a su información. Estas redes se basan en protocolos, programas y servicios diseñados a imagen y semejanza de Internet proporcionando comunicaciones interplataforma entre los usuarios autorizados.*

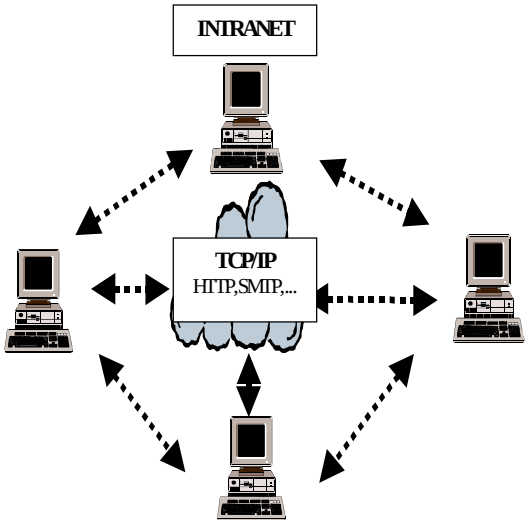

Figura 1: Intranet

La herramienta de mayor importancia en una Intranet es el **Web** , que es un servicio que se proporciona en Internet y que consiste es mostrar documentos que integran información texto, gráfica, audio y animaciones. Para crear este tipo de documentos llamados páginas Web se utiliza principalmente el lenguaje HTML y el lenguaje de programación JAVA(applets).

Definición 2 [5] [11]. *El lenguaje HTML o lenguaje de Marcas Hipertexto es un lenguaje que permite formatear información multimedia con una estructura y formato determinado. Este lenguaje se basa en marcas* ***Hipertexto****, que son elementos "resaltados" en los documentos que al seleccionarlos con un ratón u otro dispositivo apuntador nos muestran información o nos llevan a otra página relacionada con dicho elemento resaltado.*

Definición 3 [1][6]. *El lenguaje JAVA es un lenguaje de programación multiplataforma que permite crear aplicaciones interactivas repartidas por la red a través de la Web. Estos programas JAVA que se ejecutan a través de la Web es lo que se conoce como* ***Applets*** *JAVA.*

Definición 4 [6,5]. *El http es el protocolo (lenguaje de transmisión de información a través de una red de comunicaciones) utilizado en una Intranet para transmitir la información almacenada en el " servidor ", es decir, páginas HTML y applets JAVA.*
En la Intranet donde instalamos SIGEBAJA implementaremos los distintos servicios necesarios para su funcionamiento. Para poder implementar este sistema dentro de nuestra Intranet vamos a necesitar además de los protocolos y programas anteriormente mencionados tener instalado en nuestro servidor:

- Un sistema de Bases de Datos [13]. Este sistema nos proporcionará las herramientas necesarias para el mantenimiento y administración de toda la información que compondrán la Base de Datos. En ella almacenaremos las distintas preguntas del examen tipo test, además de los alumnos y profesores que forman parte de nuestro centro educativo, y por último también se almacenarán todos los exámenes realizados hasta la fecha.
- El API JDBC [7]. Esto es, un conjunto de herramientas que nos permitirán comunicarnos con la Base de Datos utilizando sentencias JAVA. Esto nos proporciona una comunicación fácil e independiente de la implementación de la Base de Datos y de los equipos que constituyen nuestra Intranet.

Una vez que hemos descrito los distintos protocolos y herramientas necesarias para la implementación de SIGEBAJA describiremos su funcionamiento:

1. Para utilizar SIGEBAJA cualquier alumno deberá de identificarse, mediante un proceso de autentificación (descrito en la siguiente sección).
2. Una vez que un alumno solicita la realización de un examen este será confeccionado en el servidor mediante un programa JAVA, el cuál se comunicará (mediante JDBC) con la Base de Datos donde se encuentran las preguntas. El examen se generará de forma aletatoria y con un número de preguntas y dificultad determinado con anterioridad por el profesor responsable mediante otro servicio proporcionado por SIGEBAJA. Las preguntas de examen se almacenarán en la Base de Datos con la siguiente estructura:
   - *Identificador de la pregunta*. Será único para cada pregunta almacenada en la Base de Datos.
   - *Pregunta*. Texto que compone la misma.
   - *Alternativas*. Se almacenará el texto de cada una de las múltiples alternativas de la pregunta.
   - *Alternativa correcta*.
   - *Dificultad*. Será necesario para confeccionar distintos exámenes de dificultad similar.
3. Una vez confeccionado el examen éste se enviará al puesto que lo solicitó y se presentará la información por medio de Applets JAVA para que el alumno pueda elegir una de las alternativas que se le proponen para cada una de las preguntas que componen el examen.
4. Una vez que el alumno termina el examen se envía de vuelta al servidor y el programa JAVA lo almacenará en la Base de Datos realizando las debidas comprobaciones de seguridad. En la Base de Datos se almacenará para cada examen: el identificativo del alumno, para cada pregunta su identificador y respuesta que el alumno marcó y por último toda aquella información de seguridad necesaria para atender posibles reclamaciones.
5. Por último se enviará al puesto cliente la nota que le corresponde al alumno en el examen.

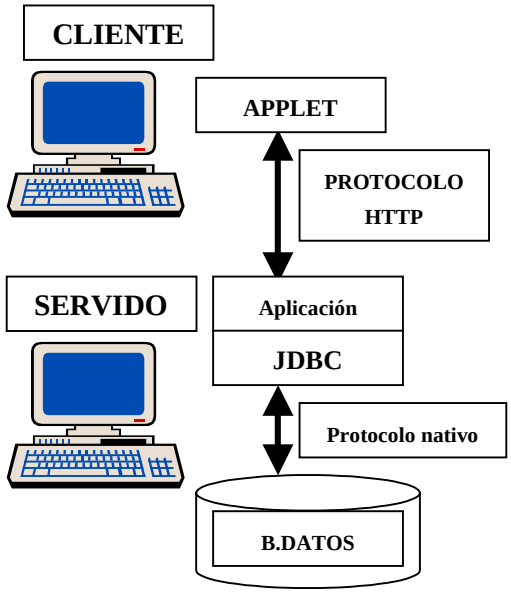

Figura 2: Comunicación en una Intranet

En la figura anterior podemos observar el esquema de la comunicación que se establece entre los

distintos elementos que componen la Intranet para dar servicio a nuestro sistema. SIGEBAJA utiliza los protocolos propios de Internet para comunicarse entre los distintos puestos y el servidor. Sólo se utilizan protocolos nativos de la Base de Datos para comunicar ésta con el programa JAVA mediante el API JDBC. La extensión de SIGEBAJA a una Extranet o Internet es inmediato ya que cualquier puesto presente en una de estas dos redes podría comunicarse mediante el protocolo HTTP con el servidor para solicitar servicio a SIGEBAJA. Lo cual nos permite utilizar el sistema para centros educativos que pretendan ofrecer la posibilidad de realizar exámenes a distancia.

4. SEGURIDAD EN SIGEBAJA

Una vez vista la infraestructura necesaria para la implantación del sistema y su forma de actuar, debemos analizar un importante aspecto como es la seguridad de SIGEBAJA. Ya que una relajación en la seguridad del sistema puede hacer que deje de ser útil para nuestros propósitos. SIGEBAJA es un sistema implantado sobre una red de ordenadores a través de la cuál se transmite información, que en nuestro caso se trata de documentos (exámenes) que pueden ser de gran importancia. Este sistema por tanto comparte los mismos problemas de seguridad que se presentan en las redes de ordenadores en general, como son: [14]

a) ***Privacidad*****:** este problema trata que la información no pueda ser accedida por personas ajenas a la organización o simplemente no autorizados.
b) ***Validación de la identificación***: se trata de determinar quién es la persona con la que se está intercambiando información antes de llevar a cabo el intercambio.
c) ***Irrefutabilidad (No Repudio):*** se encarga de la comprobación de las firmas digitales, es decir, asegurar la validez de la identificación de la firma existente en un documento
d) **Control de Integridad**: esta área se encarga de asegurar que la información que forma parte de un documento transmitido a través de una red de ordenadores no ha sido modificado a lo largo del trayecto que ha recorrido por el canal de comunicación.

Ahora particularizaremos cada uno de estos problemas sobre nuestro sistema y veremos la problemática que surge si no se pone solución.

1) ***Privacidad*****:** en nuestro sistema se manifiesta como la capacidad de poder acceder a los exámenes que viajan por la red y conocer posibles preguntas para exámenes posteriores.

2) ***Validación de la identificación:*** es fundamental determinar sin ningún genero de dudas quien es la persona que entra en el sistema para hacer el examen. La mayor dificultad en este caso es cuando el examen se realiza a distancia, ya que hay que verificar inequivocamente al alumno.

3) ***Irrefutabilidad (No Repudio):*** el sistema debe garantizar que cada examen esté totalmente identificado, para que el alumno pueda hacer cualquier tipo de reclamación sobre él excepto la de repudio, es decir, negar su autoría.

4) ***Control de Integridad:*** nuestro sistema debe garantizar que el contenido de un examen no es modificado durante su transito por la red.

Para solucionar todos estos problemas de seguridad que se dan en las redes de ordenadores se han desarrollado una serie de técnicas y políticas como son:

1) Sistemas de autentificación.

Este tipo de sistemas son una parte importante del diseño de las políticas de seguridad de cualquier sistema de redes de ordenadores. Los sistemas de autentificación lo que hacen es identificar al usuario que quiere acceder al sistema y además solicitarle una palabra clave o password *que debe ser conocida sólo por dicho usuario.*

2) Sistemas de encriptación.

La encriptación o codificación es un proceso que consiste en transformar una información expresada en un lenguaje determinado a otro lenguaje con reglas sintácticas y semánticas distintas que conserva la información anterior, pero que no puede entenderse a no ser que se conozca el proceso que realiza la función inversa, es decir, la desencriptación o descodificación. Este proceso se lleva cabo mediante un conjunto de fórmulas matemáticas complejas denominados algoritmos de encriptación.

Existen distintos métodos de encriptación o codificación:

i. *Encriptación simétrica*. Este tipo de encriptación utiliza un algoritmo para codificar y descodificar la información utilizando claves de cifrado. La idea de la clave de cifrado consiste en que si alguien codifica un mensaje, sólo alguien que conozca la clave adecuada podrá descifrarlo. El tamaño de la clave es la característica crítica de los sistemas de encriptación simétricos, dicho tamaño se cuenta en bits. El sistema

DES (Estándar de Encriptación de Datos) es el sistema más usual de encriptación simétrica en el cual tanto el emisor como el receptor necesitan conocer la misma clave secreta.

ii. *Encriptación asimétrica*. Este tipo de encriptación se diferencia del tipo anterior en que para codificar la información utiliza "un *par de claves complementarias"*: *una clave pública* y una *clave privada*. Cada elemento de la comunicación (emisor, receptor) tiene asociado una clave pública y otra privada. La clave pública está disponible libremente por cualquiera, mientras que la clave privada es conocida únicamente por su usuario propietario. Cada clave abre el código que produce la otra. Conocer la clave pública no sirve para deducir la clave privada correspondiente. La clave pública debe publicarse o al menos transferirse a quienes deseen comunicarse con nosotros de forma segura, esta publicación o transferencia puede hacerse a través de canales inseguros.

A continuación vamos a explicar como es el funcionamiento del cifrado mediante un sistema de encriptación asimétrico. Suponemos una comunicación entre los usuarios A y B. De forma que A va enviar a B un mensaje seguro utilizando codificación simétrica. A encriptará el mensaje para B utilizando la clave pública de B que bien éste le transfirió o encontró en un servidor público que contiene este tipo de información. Sólo B puede desencriptar el mensaje con su clave privada.

Estas técnicas y políticas de seguridad las aplicaremos a nuestro sistema para solucionar los distintos problemas de seguridad a los que nos enfrentamos al implantar SIGEBAJA:

1. *Privacidad:* se utilizarán sistemas de autentificación para controlar el acceso al sistema y la encriptación simétrica para guardar las palabras clave de los usuarios del sistema.

2. *Validación de la identificación:* pueden utilizarse tanto sistemas de encriptación simétricos como asimétricos para constatar la identidad de un usuario. En exámenes a distancia habría que utilizar algún medio para verificar que el alumno es el que hace el examen. Una posibilidad sería utilizar *videoconferencia*.

3. *Irrefutabilidad **(No Repudio)**:* se utiliza la encriptación asimétrica de forma que el emisor firma un examen utilizando su clave privada, el receptor (SIGEBAJA) del mensaje debe conocer la clave pública del emisor si la firma es correcta el sistema descifrará la firma con la clave pública del emisor.

4. *Integridad de la información:* también se utiliza la encriptación asimétrica. El examen se encripta usando la clave pública del sistema y todo el mensaje se codifica de forma que para leerlo se debe tener la clave privada y en caso de que haya sido modificado el contenido del mensaje al ser descifrado el sistema lo detecta.

5. CONCLUSIONES Y TRABAJOS FUTUROS

A lo largo de este trabajo hemos visto el funcionamiento del sistema SIGEBAJA y los aspectos de seguridad que hay que tener en cuenta cuando queremos utilizarlo como un sistema de exámenes reales.

En la presente comunicación el sistema presentado genera únicamente exámenes tipo test, en el futuro queremos completar la gama de generación de exámenes extendiéndola a exámenes interactivos. También pretendemos aprovechar la infraestructura instalada para el funcionamiento de este sistema para el desarrollo de otro tipo de actividades de ayuda a la formación, tal y como puede ser la atención a distancia al alumno.

Referencias

[1] Arnold ,Ken., (1997) The Java Programmin Language Second Edition. Ed. Addison Wesley.

[2] Blanco, Juan J,(1998) La Informática en el centro educativo. Una propuesta Integradora, Organización y Gestión Educativa.

[3] Carballar, José A., (1999) Internet el mundo en sus manos, Ed. Ra-ma..

[4] Coombs Ph., (1985) La crisis mundial de la educación , Perpectivas actuales. Madrid.

[5] Garret David.,(1997) Intranets al descubierto, Ed. Prentice Hall.

[6] Gralla, Preston , (1996) Como Funcionan las Intranets, Ed. Prentice Hall.

[7] Hamilthon, Graham, Cattell Rick y Fisher Maydene, (1998) JDBC Database Access with JAVA, Ed. Addison-Wesley .

[8] Loeb Larry, (1998) Secure Electronic Transactions: Introduction & Reference. Ed. Artech House Inc.

[9] Medrano, G., (1993) Nuevas tecnologías en la formación, *Ed. Eudema*.

[10] Sánchez, P., (1999) Un Sistema de Generación y Evaluación de Exámenes basado en Java. Actas del CONIED 99.

[11] Santos, G., (1997) HTML Iniciación y Referencia. Ed. McGrauw-Hill.
[12] Soon-Yong , C. (1997) Economics of Electronic Commerce. Ed. Macmillan Computer Publishing
[13] Silberschatz, Abraham Henry F. Korth y S. Sudarshan, (1998) Fundamentos de Bases de Datos, McGraw-Hill
[14] Talens, S. (1998) Internet, Redes de Computadores y Sistemas de Información