Apuestas por medio de dispositivos móviles

David Fernando Zaidiza Peñaranda, 031110

***Indice de Terminos*— Autoridad certificadora, Certificados SSL, SSL, Netbeans, WTLS, Gateway, JAR, JAD.**

I. Introducción

En el entorno de las comunicaciones se encuentran los dispositivos móviles; palm´s, Ipod´s, Celulares, etc. Un dispositivo móvil es un minicomputador que presenta características de procesamiento, almacenamiento y memoria limitada.

Para el desarrollo de este proyecto se escogió como dispositivo móvil el celular. Este posee acceso a la red de datos por medio del protocolo WAP. El dispositivo móvil celular permite el establecimiento de una conexión segura, para esto utiliza mecanismos de seguridad, tales como los certificados que brindan integridad, seguridad y autenticidad de los datos.

II. Objetivos.

A. *Objetivos específicos*

- Reconocer los algoritmos de cifrados disponibles
- Identificar cuales algoritmos de cifrado cuentan con las características para ser ejecutados en el dispositivo móvil
- Determinar el dispositivo adecuado para la implementación de la aplicación J2ME.
- Determinar el algoritmo de cifrado adecuado para un dispositivo móvil que cuente con transmisión vía celular para ser usado en juegos de apuestas de chance.
- Desarrollar una aplicación prototipo J2ME que permita realizar apuestas de chance en línea a través de un dispositivo móvil.

III. Comunicaciones

Las comunicaciones y diferentes tecnologías han permitido el progreso en la necesidad de comunicarse de las personas. Avanzando a través de las etapas en la historia; comunicación oral, comunicación escrita, la imprenta que fue creada por Johannes Gutenberg cuyo invento cambio el transcurso de la historia, ya que permitió compartir la información entre el mundo. La evolución de las técnicas de comunicación nos lleva hasta los tiempos actuales donde la transmisión de datos se realiza de manera electrónica en el área de las telecomunicaciones.

Las apuestas móviles son un nuevo mercado en el área de las telecomunicaciones, el desarrollo de la aplicación prototipo se implementó en la plataforma JAVA del dispositivo móvil celular, se utilizo el protocolo de comunicaciones WAP para realizar el envió de datos.

Para lograr la comunicación se implementa una aplicación para el celular (JAR "Java Archive" – JAD "Java Decompiler"), y una para el servidor (Servlet), en la siguiente figura se muestra la interacción Cliente-Servidor.

Fig. 1 Comunicación Cliente – Servidor

Para poder proporcionar el servicio en el servidor es necesario un mediador, TOMCAT, que es un servidor Web que trabaja con Java en entornos Web, un contenedor de Servlets y JSP "Java Server Page".

IV. Herramienta de desarrollo NETBEANS para los aplicativos Java [1]

La plataforma Netbeans es un entorno de desarrollo integrado para aplicaciones Web, el cual es utilizado para editar programas en Java, ejecutarlo, compilarlo, depurarlo entre otras opciones.

Esta plataforma se utiliza para construir el aplicativo del móvil y en el desarrollo Servlets para el servidor Web, estos dos aplicativos son utilizados para la conexión de los dispositivos.

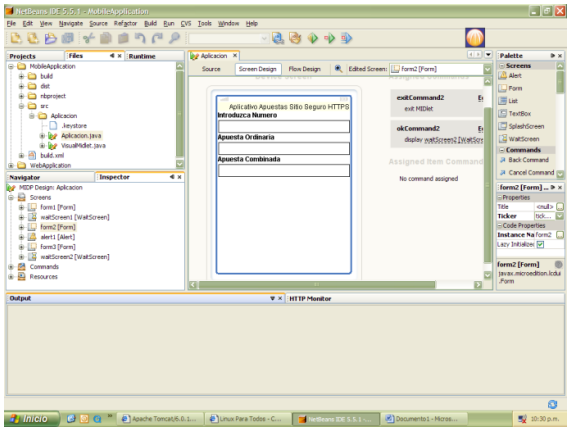

Fig. 2 Entorno de desarrollo NETBEANS

V. DESARROLLO DEL PROBLEMA.

Para este proyecto fue necesario conocer los diferentes algoritmos de cifrado existentes al igual que los dispositivos móviles disponibles capaces de soportar los mismos.
Para la selección del dispositivo móvil se tienen en cuenta las características que el sistema operativo de cada dispositivo puede ofrecer; enfoque, tecnología, adaptabilidad, compatibilidad, herramientas de desarrollo, paquetes de desarrollo y seguridad soportada.
Una vez escogido el dispositivo se procede a buscar el modo más seguro para el envió de datos por medio de la red celular.

A. *Cifrado*

En el desarrollo del aplicativo fue necesario conocer los diferentes métodos de seguridad que existen en el mercado; Algoritmos de cifrado simétrico y asimétrico cuyo desempeño esta enfocado al cifrado de información, la criptografía Hash y el firmado digital, que están enfocados al resumen de información y autenticación. [2]
Adicionalmente cada algoritmo presenta unas características que los identifican los unos de los otros como el desarrollo matemático de cada uno, un modo de empleo ya sea en bloque, por flujo de datos, firmado digital o un resumen de mensaje. [2]

B. *Dispositivo para implementar los aplicativos*

En el desarrollo del proyecto de grado se ha elegido como dispositivo móvil, el celular, ya que este presenta portabilidad e infraestructura de comunicación ya implementada. Existen gran variedad de celulares con diferentes características en los recursos, entre los cuales se encuentran los Sistemas Operativos. Estas son indispensables en la elección del dispositivo adecuado, ya que unos móviles presentan características más robustas y otras muy limitadas para la implementación de la aplicación móvil que permitirá la prueba del canal de transmisión segura. [3]-[7]

Los sistemas operativos no pertenecen solo a los PC´s, en los dispositivos móviles se encuentran gran variedad de estos, es así que en los celulares existen una variedad de sistemas operativos que no son tan conocidos como los del PC.

Fig. 3. Sistemas Operativos [3]-[7]

Dentro de los SO se encuentra Android, que es un sistema operativo el cual utiliza Linux mezclado con Java como núcleo; Iphone que se basa en OS X que es una variante de Unix, siendo Unix uno de los SO más poderosos en el mercado. Dentro de los SO más estables se encuentra Windows Mobile y S60 de Symbian, estos aparte de ser estables son SO muy maduros en cuanto a desarrollo y tiempo en el mercado.
Otro de los SO más importantes es RIM (Research in Motion) BlackBerry posee un motor de Java tal como Android.

Sistemas Operativos / Mercado		Versión del Software	Adaptabilidad	Kernel o tipo de Núcleo	Tecnología
BlackBerry	Research in Motion	BlackBerry OS 4.7	Buena	Propietario	GSM WIFI CDMA
htc Windows Mobile	Windows Mobile	Windows Mobile 6.5.	Excelente	Windows CE	GSM WIFI CDMA
palm webOS	PalmOS	Palm WebOS	Excelente	Linux	GSM WIFI CDMA
symbian	Symbian	S60	Excelente	Symbian	GSM WIFI
android	Linux	Android con Cupcake	Excelente	Linux	GSM WIFI
Sony Ericsson	Sony Ericsson Propietario	MIDP 2.1	Excelente	Propietario	GSM WIFI
	Mac OS X	iPhone OS 3.0	Mala	OS X	GSM WIFI

Fig. 4.caracteristicas de los Sistemas Operativos

Para poder seleccionar el dispositivo móvil adecuado se deben tener en cuenta todas las características que proporciona cada sistema operativo. [3]-[7]

- Enfoque en el que desarrollo el dispositivo
- Tecnologías soportadas
- Adaptabilidad
- Compatibilidad
- Herramientas de desarrollo
- Paquetes de desarrollo
- Seguridad soportada

	Enfoque	Tecnología	Adaptabilidad
Symbian	Aplicativos unificando un solo sistema operativo	Compatible	Excelente
Sony Ericsson Propietario	Aplicativos para un sistema operativo basado en Java	Compatible	Excelente
Amdroid	Software libre	Compatible	Excelente
Mac OS X	Entretenimiento	Compatible	Mala
BlackBerry	Empresarial	Compatible	Buena
Palm OS	Empresarial	Compatible	Excelente
Samsung Propietario	Aplicativos compatibles con J2ME	Compatible	Excelente
Windows Mobile	Empresarial	Compatible	Excelente

Fig. 5. Tabla de Características I

	Compatibilidad	Herramientas de desarrollo	Seguridad soportada
Symbian	MIDP 2.0	Netbeans Mobility Pack4.0 Eclipse ME j2ME Development for Eclipse 3.0	Algoritmos de cifrado – llaves hash – certificados –firmado digital
Sony Ericsson Propietario	MIDP 2.0	Netbeans Mobility Pack4.0 Eclipse ME j2ME Development for Eclipse 3.0	Algoritmos de cifrado – llaves hash – certificados HTTPS – firmado digital
Amdroid	MIDP 2.0	Netbeans Mobility Pack4.0	Problemas de seguridad
Mac OS X	MIDP 2.0	Flurry	Problemas de seguridad
BlackBerry	MIDP 2.0	Mobil Data System v4.1	Algoritmos de cifrado – llaves hash – certificados HTTPS
Palm OS	MIDP 2.0	Sun Java Studio Mobility	Algoritmos de cifrado – llaves hash – certificados HTTPS
Samsung Propietario	MIDP 2.0	Sun Java Studio Mobility Netbeans Mobility Pack4.0	Algoritmos de cifrado – llaves hash
Windows Mobile	MIDP 2.0	Sun Java Studio Mobility Eclipse ME j2ME Development for Eclipse 3.0	Algoritmos de cifrado – llaves hash – certificados HTTPS

Fig. 6. Tabla de Características II

C. Implementación de la seguridad en el dispositivo móvil [3]-[9]

En la seguridad móvil se debe tener en cuenta varios aspectos, tales como la forma de transmisión segura y el modo de implementación de esta. Los beneficios que ofrece actualmente la tecnología móvil nos permite tener al alcance servicios de Internet Móvil, dando la posibilidad de realizar diversas operaciones transaccionales. Esto se puede llevar a cabo gracias a la tecnología WAP; este en un estándar que permite el acceso a Internet desde terminales móviles. Los creadores de dicho protocolo son Ericsson, Motorola, Nokia y Unwired Planet. [2]

El objetivo principal de la conexión a Internet móvil es poder comunicarse con el fin de compartir información con usuarios en el mundo sin tener limitaciones de movilidad. La cuestión es que no toda la información que viaja vía Internet la puedan tener al alcance usuarios no deseados. La tecnología WAP es escalable permitiendo que las aplicaciones dispongan de la capacidad que brinda cada pantalla de los dispositivos móviles; recursos según la necesidad. [8], [9]

SSL Secure Sockets Layer, es un protocolo diseñado por Netscape Comunications Corporation con el fin de brindar seguridad a las sesiones de navegación a través de la red de Internet. [8] Este proporciona servicios tales como:

- Confidencialidad

Aquí se encuentra la seguridad por medio del cifrado de datos, se garantiza que la información transferida es indescifrable para personas ajenas al objetivo del mensaje. El cifrado que se utiliza es criptografía de clave simétrica con una clave se sesión que se acuerda mientras se establece la conexión, verificando la identidad de las partes y determinado los parámetros que se utilizaran.

- Autenticación

El usuario puede estar seguro de la identidad del servidor, al cual se conecta y valida con el fin de intercambiar información de manera confiable. Esto se hace mediante certificados basados en criptografía de clave pública. Por lo general el que se autentica es el servidor mediante un certificado digital.

- Integridad

No se permite modificar el mensaje mientras viaja a través de la red de Internet. Esto lo hace utilizando códigos de integridad, los cuales se calculan utilizando HASH (SHA – MD5). [8]

La implementación de la aplicación segura cliente - servidor en la red celular se realiza de la siguiente manera:

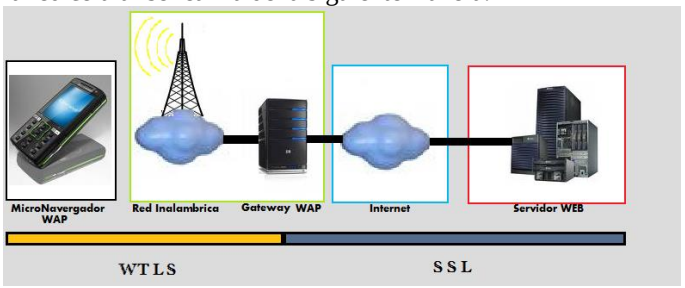

Fig. 7. Comnicacion segura Cliente – Servidor

El modelo consta de tres partes:

- El Gateway Wap utiliza SSL (Secure Sockets Layer) para realizar la comunicación de manera segura con el servidor WEB. Brindando privacidad, integridad y autenticación del servidor. [9]
- Para la comunicación entre el Gateway y el dispositivo móvil celular utiliza WTLS (Wireless Transport Layer Security). [9]
- El puente entre los protocolos SSL y WTLS es el Gateway WAP. [9]

Se implementa un certificado SSL para poder realizar la comunicación segura basada en el modelo de la Fig. 8. Un certificado permite el cifrado de información confidencial durante transacciones en línea, cada certificado contiene información exclusiva y autenticada sobre el propietario del certificado. Una entidad de certificación verifica la identidad del propietario del certificado cuando se emite.
Se utiliza un certificado SSL cuando se tiene una tienda electrónica o se reciben tarjetas de crédito en línea, cuando se inicia la sesión de un sitio Web, al procesar datos confidenciales como direcciones, identificaciones nombre. Un certificado establece un canal de comunicación privado permitiendo cifrar los datos durante la transmisión proporcionando la confidencialidad de los datos. [8]

Los certificados SSL constan de una clave pública y una clave privada. La clave pública es utilizada para cifrar la información y la privada para descifrarla. Al conectarse a un dominio desde un navegador WEB una presentación SSL autentica al servidor WEB y al cliente o navegador WEB. Se establece una clave de sesión exclusiva con el fin de iniciar la conexión segura.

El diagrama del aplicativo diseñado es el siguiente, este es el que implemento en el dispositivo móvil celular. El cual se conectara al servidor por medio del protocolo WAP.

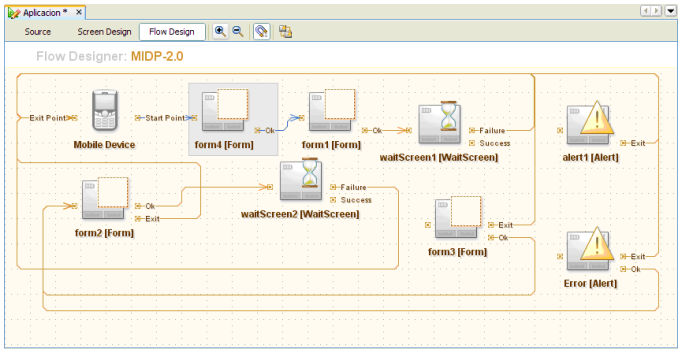

Fig. 8. Diagrama del aplicativo

En cuanto al servidor se puede verificar la seguridad de la conexión mediante al certificado creado para la página https://www.zaidiza.com/conection.jsp, siendo esta la misma pagina a la cual esta diseccionado el aplicativo móvil celular.

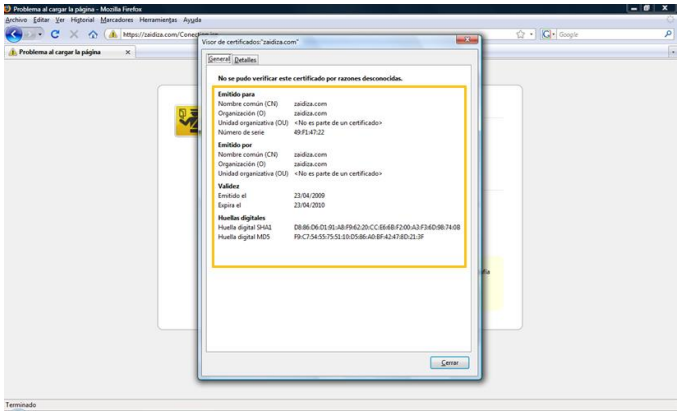

Fig. 9. Certificado SSL

VI. Conclusión

- Existen gran variedad de algoritmos de cifrados, pero no todos son factibles de implementar en dispositivos móviles. La implementación de los algoritmos depende del fabricante del sistema operativo, ya que este define las características del dispositivo; seguridad, adaptabilidad, los paquetes de desarrollo y hacia qué mercado está enfocado el dispositivo.
- La determinación del dispositivo para la implementación de una aplicación prototipo móvil, depende de las características y configuraciones que el sistema operativo brinde al desarrollador. Para el caso de este proyecto, el sistema operativo más óptimo es el Sony Ericsson Propietario.
- Al implementar un canal seguro no basta solo con cifrar la información, se requiere de una entidad que permita autenticar que la información que ha llegado al destinatario por medio de la red de datos celular.
- Al determinar la forma de transmisión segura se garantiza que los datos llegan de manera confiable, íntegra y autenticada. Esto se logra por medio del certificado SSL que garantiza tres aspectos, confidencialidad por medio de los algoritmos de cifrado, autenticación identificando el servidor e integridad de los datos no permitiendo que los datos sean modificados ni leídos por terceros.
- Teniendo en cuenta que existe gran variedad de dispositivos móviles en el mercado, se concluye que la unificación de un sistema operativo aún está lejos, las diferencias de diseño, perfil, requerimientos y características de cada compañía aún no permiten crear un perfil único.
- El desarrollo del aplicativo móvil demuestra que la transmisión de datos seguros por medio de dispositivos móviles en la red celular es posible.

RECOMENDACIONES

Al realizar una conexión segura se debe tener en cuenta como primer campo los diferentes sistemas operativos existentes en el mercado, ya que será uno de los parámetros para escoger el dispositivo donde se implementará el aplicativo. El sistema operativo define compatibilidad y adaptabilidad del mismo, según este se puede ver que tan viable es desarrollar una aplicación para un móvil.

Al escoger la forma de envió de datos se debe tener en cuenta que no solo se debe garantizar que los datos viajen seguros si no que adicionalmente se debe poder ofrecer datos confiables, no modificados por terceros y que provengan de una fuente segura y certificada.

Los servicios que ofrezcan el aplicativo se definen según el cliente, ya que el objetivo principal de este proyecto de grado es el envió de datos de manera segura por medio de un dispositivo móvil.

En una transmisión segura con certificados SSL se garantizan tres aspectos, confidencialidad, autenticación e integridad de los datos.

TRABAJO A FUTURO

En la visión de trabajo a futuro se encuentra desarrollo de aplicativos que permita tener funcionalidad en empresas según sus requerimientos. Garantizando así un canal ciento por ciento seguro, además de ser certificado. La posibilidad de implementar la una combinación de algoritmos que permita garantizar el envío de mensajes entre emisor y receptor con un grado más alto de seguridad.

Permitir el desarrollo de nuevos servicios según el requerimiento del cliente, tal como una interfaz de estadística dinámica con datos obtenidos en línea, como apuestas, cantidad de jugadores, jugadas.

Agradecimientos

Durante el desarrollo de mi carrera he encontrado constates obstáculos, los cuales han sido superados gracias a la aparición de personas valiosas personas en mi camino hacia el éxito. La variedad de situaciones que te ponen a prueba permiten el forjamiento de un carácter y disciplina que será indispensable en el comienzo del vivir, es así que la mejor manera de agradecer a esas personas no es con palabras si no con acciones de logros.

Doy gracias a mi madre quien con sus manos labro un camino el cual seguir, mi familia quien creyó y apoyo la decisión de crecer en conocimiento, a mi padre quien me enseño el tener visón y

en especial a esa persona que forjo mi persona, esa que mostró que la experiencia es importante, que el conocimiento se transmite y que puede ser vivido, gracias a mi abuela Orfelina.

Finalmente agradezco a mi asesor quien afronto el reto de tomar este proyecto y guiar mi ambición.

REFERENCIAS

[1] DECSAI Universidad de Granada (2006,Sep,1) Curso de formación continua de programación de dispositivos móviles Java (4a edición) [PDF]Disponible: http://leo.ugr.es/J2ME/APPS/GuionTetris/guionNetbeansMoviles.pdf

[2] Schneier, Bruce. Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd. Edition. John Wiley & Sons, 1996.

[3] ENGADGET en español (2009,Mar,19) La gran comparación de los sistemas operativos móviles [En línea] Disponible: http://es.engadget.com/2009/03/19/la-gran-comparacion-de-los-sistemas-operativos-moviles/

[4] Huidobro Moya,Jose Manuel. *Comunicaciones Móviles.* Ed. Thomson-Paraninfo. Glosario: Págs. 419-431

[5] Milenkovic Milan, (1993), "Sistemas Operativos Conceptos y diseño", Ed. Mc Grw Hill España.

[6] Stallings William, (2001), "Sistemas operativos",Ed. Prentice hall

[7] Deitel Harvey M., 1993, "Sistemas operativos", Ed. Addison.

[8] VERISING (1995-2009) Certificados SSL [En línea] Disponible: http://www.verisign.es/ssl/ssl-information-center/how-ssl-security-works/index.html

[9] Dornan, Andy. *WAP*. Ediciones Anaya Multimedia. Glosario: Págs. 319-336.

David Fernando Zaidiza Peñaranda, 031110. Proyecto de Grado para la Fundación Universitaria San Martín.