Análisis y descripción de la gestión de la seguridad en ambientes UMTS y desarrollo de herramienta didáctica

Nicole Valverde P., Iván Farez T., M.Sc. Washington Medina
Facultad de Ingeniería en Electrica y Computación.
Escuela Superior Politécnica del Litoral (ESPOL)
Campus Gustavo Galindo, Km 30.5 vía Perimetral
Apartado 09-01-5863. Guayaquil-Ecuador
nicsaval@espol.edu.ec, ifarez@espol.edu.ec, wmedina@espol.edu.ec

Resumen

Este trabajo de investigación está enfocado a la seguridad en redes UMTS y la creación de una aplicación web, ya que es una herramienta poderosa que muchas personas pueden acceder libremente, debido a que resulta complicado encontrar material didáctico en el tema de seguridad celular, además que muchas veces la información que se necesita se encuentra en otros idiomas complicando el aprendizaje, resultando ser material muy extenso y complejo de interpretar.

Por eso se pensó en la necesidad de una herramienta didáctica que vaya al alcance de las nuevas tecnologías (internet), el cual se encuentra disponible en todo el mundo, sin restricciones además de tener material resumido y en la lengua nativa, en español, así las personas puedan introducirse de a poco en el tema de seguridad, ya que poco o nada se sabe generalmente sobre ella, y el acceso a estos contenidos solo lo obtienen las personas preparadas y dedicadas a dicho estudio.

En los cuatro primeras secciones se muestra un resumen de temas que tratan sobre seguridad en ambientes UMTS, en la primera se enfatiza sobre la historia y arquitectura de la red UMTS, el segundo describe la arquitectura IMS, mientras que en el tercera y cuarta sección explican sobre algoritmos de cifrado y métodos utilizados en las redes UMTS para protección de los datos. La última sección muestra el desarrollo de la aplicación web, su arquitectura y su diseño.

Palabras clave: *UMTS, 3G, Seguridad, Aplicación.*

Abstract

This research is focused on security in UMTS networks and the creation of a web application as it is a powerful tool that many people can freely access because it is difficult to find teaching materials on the topic of mobile security, in addition to the fact that often the information you need is in other languages, complicating learning, proving to be very extensive material and hard to interpret.

So, it has thought of the need for an educational tool to be according to the reach of new technologies (internet), which is available worldwide, unrestricted, besides having summarized material in the native language, Spanish, and people can be introduced slowly in the security topic, since little or nothing is generally known about it, and the access to this content is only obtained by people who are prepared and dedicated to such study.

In the first four sections a summary of issues dealing with security in environments UMTS is shown, the first one emphasizes on the history and architecture of the UMTS network, the second describes the IMS architecture, while the third and fourth section explain about encryption algorithms and methods used in UMTS networks for data protection. The last one shows the development of web application, its architecture and design.

Keywords: *UMTS, 3G, Security, Application.*

1. Introducción

UMTS (Universal Mobile Telecommunication System), estándar europeo de tercera generación, es una mejora al antiguo sistema GSM, ya que utiliza muchos conceptos de dicha tecnología, por lo que se pueden interconectar distintos dispositivos. UMTS se creó en base a un estándar con el objetivo de poder adaptar varios servicios dentro de la misma red.

Una de sus características que supera a la antigua tecnología de segunda generación es que la tasa de bits para transmisión, teóricamente llega a 2 Mbps, lo que permite la transmisión en tiempo real de audio y video, además de permitir que se trabaje con otras aplicaciones IP con el fin de que su calidad de voz sea equiparable o superior con la red de telefonía fija. Otra diferencia considerable es su tipo de modulación, GSM es basado en TDMA mientras que UMTS se basa en

WCDMA (Wideband Code Division Multiple Access) de espectro extendido, es decir, que los usuarios transmiten simultáneamente sus datos y llamadas sobre varias frecuencias al mismo tiempo con el mismo ancho de banda puesto no hay separación de frecuencia, además de ser espectro extendido en su banda base en la salida de su origen para esparcir la señal en todo el ancho de banda por seguridad, mientras que los usuarios TDMA usan un canal fijo para cada transmisión durante un intervalo de tiempo.

UMTS es capaz de interactuar con sistemas de Segunda Generación (2G), permitiendo una suave transición hacia los sistemas de tercera generación; por lo que aún el sistema GSM es importante y continuará trabajando en paralelo con UMTS por algún tiempo. Sin embargo, utilizan diferentes bandas de frecuencia: UMTS trabaja en las bandas de 1920 – 1980 y 2110 – 2170 MHz para enlaces de subida y de bajada con duplexacion FDD, WCDMA, con una longitud de 5 MHz de canal y separación entre ellas de 200 KHz. Bandas de 1900 – 1920 y 2010 – 2025 MHz para duplexacion TDD, CDMA con longitud y separación de canal similares. Finalmente bandas de 1980 – 2010 y 2170 – 2200 MHz para enlaces de subida y bajada satelitales [1].

El sistema UMTS integra todos los servicios ofrecidos por las distintas tecnologías precedentes y redes actuales, incluyendo Internet. Este sistema se compone de 3 grandes bloques que se los describirá en su momento:

- Red central o núcleo de red (Core Network, CN)
- Red de acceso de radio (Radio Access Network, RAN ó UTRAN)
- Terminales móviles (User Equipment, UE) [2].

En el lado de seguridad, muchas técnicas de cifrado se han propuesto para aumentar la seguridad UMTS; sin embargo en los inicios de ésta tecnología no fue posible decidir entre diferentes propuestas y opciones por las limitaciones impuestas por la arquitectura del sistema de ese entonces.

Por estos inconvenientes se necesitaba de alguna organización que se encargue de poner en marcha y agilice los planes de actualización de la tecnología móvil, lo que dio origen al Proyecto asociación de tercera generación (3GPP), organización de grupos, creado principalmente para diseñar un protocolo para un sistema global de telecomunicaciones de tercera generación 3G en dispositivos basados principalmente en GSM.

2. Arquitectura IMS para asegurar el acceso

Una parte importante del grupo de trabajo 3GPP se encuentra enfocado a la especificación de la IP Multimedia CN Subsystem (IMS). Es un sistema de la capa de aplicación que utiliza PS de dominio, pero está diseñado de tal manera que es independiente de la tecnología de acceso subyacentes como son los sistemas UTRAN y GERAN, bases para las redes UMTS y empezar a utilizar diversos servicios multimedia mediante IP [3].

IMS es una plataforma que permite conectividad sobre infraestructura IP entre los dispositivos que posean una dirección IP única, compatible con IPv6, ya que no tiene escasez de direcciones como es el caso de IPv4. Además de soportar tráfico de voz y datos, como es el caso de GSM, también permite voz sobre IP (voIP), servicios multimedia avanzadas para todo terminal ya sea móvil o fijo que se pueda conectar a la red con alguna dirección IP, y mantenimiento de las sesiones sin importar que haya cambio de red u operadora.

La arquitectura IMS es basada en SIP (Session Initation Protocol) desarrollado por IETF, la cual brinda iniciación, mantenimiento, registro y culminación de sesiones IMS, además de especificar la ubicación de sus usuarios conectados. Para proteger la integridad de estos servicios, se usa el protocolo SPD (Session Description Protocol) de IPsec (en especial los mensajes INVITE utilizados para establecer sesiones) entre los extremos para decidir qué tipos de formatos multimedia entrarán en la sesión como se observa en la figura 1.

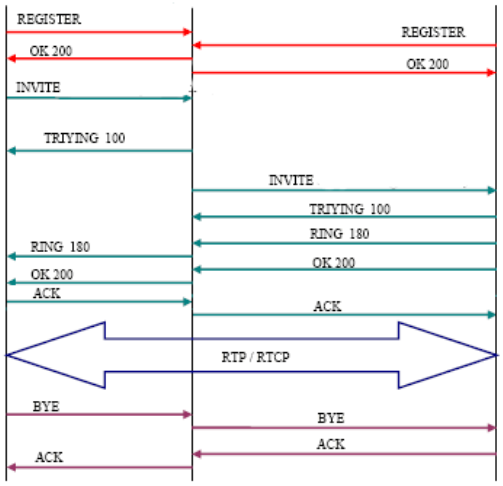

Figura 1. Autenticación SIP

Un usuario o Agente de Usuario (UA) inicia la sesión por medio de la petición INVITE, el agente SIP, intermediario de dichas peticiones, ayuda a autenticar los mensajes SIP e intercambiar datos multimedia entre los extremos, así como también

enviar peticiones de REGISTER a un servidor de registro SIP, el cual guarda información relacionada con el usuario y su sesión con la finalidad de que otros usuarios lo puedan encontrar, o si ya no quiere ser encontrado puede borrar su registro. El usuario destino acepta la invitación con el mensaje OK para establecer la llamada e intercambio de datos de voz en tiempo real mediante el protocolo para el transporte de datos RTP (Real-time Transport Protocol) y al terminar el intercambio o la sesión, cualquiera de los usuarios puede enviar el mensaje de BYE. Pero no solo hay estas peticiones, igualmente hay la petición OPTION para conocer las opciones del usuario que establece la sesión sin inicialarla previamente, ACK y CANCEL para confirmar y denegar dichas sesiones respectivamente [4].

3. Tipos de algoritmos de cifrado

En redes UMTS, existen dos tipos de cifrados, una es cifrado por bloques (Block Ciphers), el cual utiliza los códigos de autenticación de mensajes para demostrar la integridad del mismo y como método de autenticación de la entidad receptora; y el otro tipo es cifrado de flujo de transmisión (Stream Ciphers), que son utilizados para la voz y los datos.

3.1. Cifrado de flujo de transmisión (Stream Ciphers)

El cifrado de flujo es un algoritmo criptográfico para el control de la confidencialidad, con el objetivo de cifrar un texto plano. De manera similar que en cifrado de bloques, dicho texto se convierte de cadena de datos en una cadena de bits, que luego es combinada con una secuencia de bits de clave (keystream) mediante la operación XOR, que resulta en un flujo de texto encriptado. El proceso de descifrado que ocurre en el otro extremo, se lo hace de manera inversa, desligando el flujo de texto plano con el flujo de claves, haciendo sus algoritmos de cifrado y descifrado idénticos [4].

3.1.1. Algoritmo de confidencialidad f8

El algoritmo de confidencialidad f8, utilizado para cifrar y descifrar los bloques de texto, en el dispositivo del usuario, a partir de una clave CK previamente calculada durante la autenticación, calcula una secuencia de cifrado para luego realizar una operación XOR entre esta secuencia de bits y los datos originales, obteniendo un bloque de datos cifrados, los cuales se envían a la red a través de la interfaz radio. Mientras en el RNC, se realiza una operación XOR entre esta secuencia y el bloque cifrado recibido para así recuperar los datos originales.

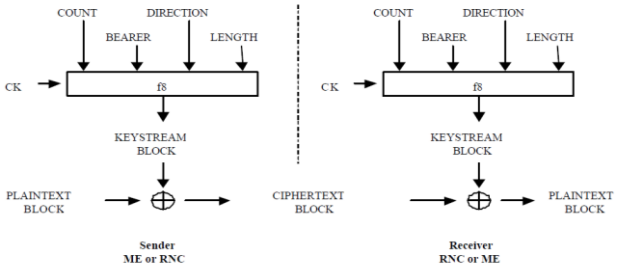

Figura 2. Mecanismo de control de confidencialidad UMTS

Las ventajas de este tipo de criptografía es su rapidez y menor complejidad de hardware para su implementación. Además de que éste algoritmo puede ser adaptado para que procese el texto plano bit a bit sin propagación de errores [4].

El algoritmo f8 hace uso de un cifrado de bloques KASUMI desarrollado para este fin por el grupo de trabajo algoritmos 3GPP. KASUMI es una modificación de MISTY1 y ofrece un grado de seguridad alto.

3.2. Cifrado de bloques (Block Ciphers)

El cifrado en bloque trabaja con el texto en claro que es separado en grupos de bits de igual longitud denominados bloques, y a cada bloque se le realiza una transformación XOR con la clave secreta, resultando en bloques de texto cifrado de igual tamaño. De ésta manera se forma el primer bloque de cifrado, donde el bloque de texto cifrado se suma con el segundo bloque de texto plano para luego encriptar su resultado con la clave secreta, y continúa sucesivamente hasta cifrar todos los bloques.

El algoritmo de control de integridad f9 de cifrado por bloques garantiza la integridad de la información de señalización para el usuario como para la red y su estructura es de cifrado por bloques, mientras que una de las funciones principales del algoritmo de cifrado de flujo f8 es la de evitar que la identidad de algún usuario que recibe determinados servicios pueda extraerse de la conexión en la que se encuentra como también de su ubicación [5].

3.2.1. Algoritmo de integridad f9

Dado que el control de la información de señalización transmitida entre la estación móvil y la red es tan importante, su integridad debe ser protegida. El mecanismo que lleva a cabo esta función de seguridad se basa en un algoritmo de integridad f9 (arquitectura vista en la Figura 3) implementado tanto en la estación móvil como en el módulo de la UTRAN más cerca de la red de núcleo, es decir, el RNC.

Para verificar el origen e integridad de los mensajes recibidos, el receptor calcula el MAC-I y compara con el recibido con el mensaje de señalización, descartando los que tengan un código MAC diferente. Este checksum se lo realiza con el algoritmo de integridad UMTS f9, el cual usa una clave IK de 128 bits durante el procedimiento de autenticación.

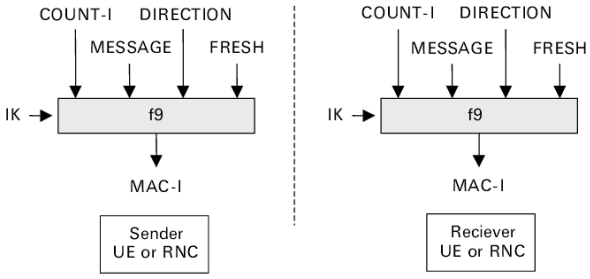

Figura 3. Algoritmo de cifrado f9

La versión final del algoritmo de cifrado de bloques se conoce como KASUMI, que en japonés significa "nebuloso, oscuro, confuso". KASUMI, también llamado A5/3, es una unidad de cifrado por bloques utilizada en algoritmos de confidencialidad f8, e integridad f9 para Telefonía móvil 3GPP.

3.3. Estructura del algoritmo KASUMI

El algoritmo de cifrado KASUMI, de bloques de salidas de 64 bits con claves de 128 bits, presenta una estructura de Feistel por su antecesor MISTY, comprendido en ocho rondas, el cual la entrada de texto sin formato es la entrada a la primera ronda y el texto cifrado luego de la vuelta final, el cual se lo puede observar en la Figura 4; la codificación y decodificación son parecidas pero con claves K diferentes (KLi, KOi y KIi) en cada ronda i, con una función diferente [6].

La función FO, llamadas redes internas donde cada una tiene tres rondas que hace uso de la subfunción FI, las subclaves (KOi, KIi), la función FL, el cual consta de una entrada de 32 bits y la subclave KLi que es dividida en dos subclaves más de 16 bits (KLi1 y KLi2).

En la estructura en cada iteración separa el bloque de un mensaje en dos partes o funciones de 32 bits: una derecha (FO) y otra izquierda (FI), conmutando éstas partes con una función unidireccional, por un número reiterado de veces. Sin olvidar que el orden de las subfunciones depende del número de iteración, es decir, en rondas pares se aplica primero la función FO mientras que en las impares la función FI es asignado primero [6].

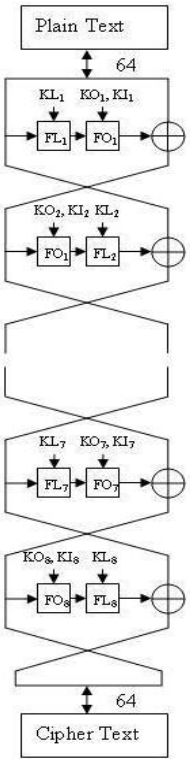

Figura 4. Cifrado por bloques KASUMI

4. Algoritmos de autenticación y generación de claves

Para que haya comunicación entre las diferentes aplicaciones, USIM y el AuC, es necesario un algoritmo estándar para la interoperabilidad, característica indispensable que debe brindar un servicio móvil de tercera generación.

4.1. Algoritmos de Autenticación de claves

El sistema AKA de UMTS tiene diferentes tipos de algoritmos criptográficos para realizar varias tareas de seguridad. En total ocho funciones diferentes son usados, aunque dos de éstas (f5 y f5*) son opcionales:

- f0, función de generación de desafío aleatoria
- f1, función de autenticación de red
- f1*, función de autenticación de mensajes de re-sincronización
- f2, función autenticación de usuario (AUTN)
- f3, clave de cifrado (CK) función de derivación
- f4, integridad de claves (IK) función de derivación
- f5, clave de anonimato (AK de 64 bits) función de derivación para el funcionamiento normal (opcional)

- f5*, clave de derivación de AK para la re-sincronización (opcional)

Las funciones f1 al f5, f1* y f5* están localizadas en las AuC y el USIM, mientras que la función f0 solo se las asigna al Auc [4].

4.2. Proceso para autenticación y acuerdo de claves

El objetivo de este proceso es el de autenticar al usuario y establecer un nuevo par de claves de integridad y cifrado entre el VLR y el USIM de usuario. Para obtener la autenticación mutua entre el usuario y la red con el conocimiento de una clave secreta K solo para el USIM y el AuC del abonado, el VLR/SGSN manda una petición al AuC, éste en respuesta envía una cadena ordenada de n vectores de vuelta al origen que sirven para una correcta autenticación y acuerdo de claves entre el VLR/SGSN y el USIM.

El HLR/AuC genera un número aleatorio RAND con ayuda de la función f0 que calcula la MAC para MAC-A, la salida XRES de la función f2, la clave CK de la función f3 y la clave IK de la función f4; le agrega el símbolo de autenticación AUTN que contiene el SQN, AMF y el MAC-A, con lo que forma el "quinteto" Q = (RAND, XRES, CK, IK, AUTN), llamado también como "Vector de autenticación". En el caso de que la SQN esté oculto, el HLR/AuC puede calcular esta clave AK de la función f5 (de manera opcional), con lo que la función de autenticación del usuario (AUTN) contendría los mismos elementos aunque el SQN se le sumaría la clave AK.

En ese momento que recibe dichos parámetros, el USIM recupera el SQN oculto si es que estuviese oculto, y valida el AUTN recibido, y si es correcto genera una respuesta RES que es enviada de vuelta al VLR con las claves CK e IK calculados con los otros vectores. El VLR compara la respuesta esperada RES o XRES y si es afirmativa, éste considera el proceso finalizado con éxito; con lo que las claves IK y CK se envían desde las dos aplicaciones (VLR y el USIM) hacia las entidades que ejecutan las funciones de integridad y confidencialidad o cifrado [5].

4.3. Algoritmo MILENAGE

Para la realización del cálculo del vector de autenticación se usan cinco funciones, denotadas por f1, f2, f3, f4, f5, y la elección de cualquiera es específica del operador, debido a que solo se usan en las AuC y las tarjetas SIM. Pero para lograr interoperabilidad entre el AuC y las distintas implementaciones del USIM podría requerir un esfuerzo extra; por lo que facilitaría el proceso si se utilizara un algoritmo estándar.

En la tecnología 3G, para evitar el inconveniente, el grupo 3GPP crearon un conjunto de algoritmos de autenticación y generación de claves (AKA) denominado MILENAGE, encaminado hacia los operadores que no desean proveer alguno de su propiedad, ya que el diseño e implementación de algún algoritmo de cifrado es complejo además de costoso y no se encuentra al alcance de todas las operadoras [4].

Su arquitectura es tan flexible, que permite a los operadores definir y gestionar su propio valor para OP, valor que será utilizado en cada módulo USIM de sus suscriptores. Dada su importancia en el proceso de autenticación, 3GPP decidió colocar un valor intermedio no invertible llamándolo OPc, dependiente de cada abonado, almacenando dentro de ella el valor de OP y la clave secreta K (OPc = OP + Ek(OP)), haciendo más difícil a algún atacante deducir el valor de OP aún teniendo un gran número de OPc y claves K. Aunque se recomienda que éste valor se mantenga en secreto, el algoritmo MILENAGE está diseñado que aún sabiendo el valor de OP en el criptoanálisis, la plataforma sigue siendo segura; es decir, que el cifrado de la OP proporciona un nivel adicional de seguridad, siendo un obstáculo más en la trayectoria del atacante [7].

4.4. Compatibilidad con A3/A8

La red GSM utiliza dos algoritmos relacionados, A3 y A8, para autenticar al suscriptor (A3) y para generar una clave de cifrado (A8). Al igual que las funciones de autenticación UMTS (f1-f5), los algoritmos A3/A8 son específicos de los operadores e implementados en la tarjeta SIM independiente del hardware o la operadora. Esto quiere decir que si un terminal UMTS visita una red que sólo admite la autenticación y cifrado GSM, el terminal debe autenticarse utilizando la interfaz A3/A8 para su conversión (las entradas de f1-f5 para salidas A3/A8) y lo contrario cuando desea entrar a una red 3G: se utilizan las reglas de conversión para las entradas A3/A8 a las salidas f1-f5 [8].

Estas reglas de conversión también se pueden utilizar junto con los algoritmos MILENAGE para aplicarse en tarjetas SIM GSM como viceversa.

4.5. Proceso de compatibilidad con A3/A8

el algoritmo A3 se utiliza para la autenticación del usuario a la red mientras que el otro algoritmo A8 se usa para generar la clave de sesión Kc y la clave SRES. Estos parámetros van hacia la red con la que se quiere autenticar después de que dicha red haya enviado el desafío para el reconocimiento del usuario. Después de su autenticación por parte del usuario, puede ordenar al móvil comenzar la encriptación usando la clave de sesión Kc para tener una transferencia de voz y datos segura [8].

El sistema de seguridad de GSM constituyó un punto de partida para el desarrollo de las funciones de seguridad de las generaciones siguientes. Su objetivo inicial fue el de garantizar la correcta facturación de las llamadas telefónicas utilizando diversos mecanismos de autenticación seguros, ya sea por medio de la clave secreta almacenada en el SIM o protegiendo el enlace por dónde va el mensaje y proteger la autenticación del abonado.

Aunque la red GSM tiene muchas fallas en el tema de seguridad, siendo una debilidad que puede ser ventajosa para ser utilizado por algún atacante externo que desee causar daño al usuario o la red misma. Por tal motivo, fue de mucha importancia mejorar la seguridad de extremo a extremo para satisfacer con la necesidad de tener un sistema que vaya acorde con la demanda mundial de servicios móviles rápidos y con el desarrollo de las funciones de seguridad, de futuras aplicaciones y tecnologías para tecnologías de tercera generación como lo es UMTS y sus posteriores.

UMTS es una ya una tecnología que se encuentra posicionada, contando con millones de usuarios a nivel mundial y continúa en aumento, además de poseer una gran cantidad de equipos para su operación, está evolucionando, desarrollándose y muchas compañías proveedoras de servicios móviles siguen impulsándola, mejorando sus protocolos de seguridad y ofreciendo un mejor servicio a sus usuarios. En el trabajo escrito se describe con más detalle, al igual que en la página web desarrollada, los elementos y servicios que ofrece esta red de tercera generación [9].

5. DESARROLLO DE LA APLICACIÓN WEB

Para el diseño de la herramienta didáctica se ha utilizado una aplicación web, la cual la hemos llamado LUS (Learning UMTS Security), un medio por el que cualquier usuario con acceso a internet puede acceder, además de ser netamente dinámica explicando detalladamente algunos temas de la seguridad en UMTS y el proceso en el cual se genera cada uno de los temas a tratar.

Una de las ventajas de presentar una aplicación web es que los estudiantes podrán tener un extenso material, además de la visualización de los diferentes temas en lo que se refiere a la seguridad en redes UMTS, sus procesos de autenticación, arquitectura, información sobre las redes precedentes a ella, historia y evolución de las redes móviles hacia la tercera generación 3G.

En “LUS” los visitantes se pueden registrar, leer el contenido del sistema, realizar pequeñas revisiones del capítulo si desean llamadas “Lecciones”, observar su puntuación de las lecciones.

5.1. Lenguaje de Programación

Python es un lenguaje de programación flexible, de fácil entendimiento y multiparadigma, es decir, no obliga a los programadores a adoptar un estilo particular de programación, permite varios estilos: programación orientada a objetos, programación imperativa y programación funcional.

Figura 5. Logo de Python

Python es una herramienta tan poderosa que se puede usar en desarrollo web, para escribir interfaces gráficas de usuario (GUI) de escritorio, crear juegos relativamente con gran facilidad y claridad de código [10].

5.3. Framework

Para la creación de una aplicación web de manera fácil, ordenada y segura generalmente los programadores utilizan herramientas de desarrollo para no tener que volver a escribir funciones para tareas de sistemas ya creadas. Para esto se utilizó un framework web.

Un framework es una plataforma para el desarrollo de aplicaciones de software. Proporciona una base estructurada sobre la que los desarrolladores de software pueden crear programas.

5.3.1. Django

Django es un framework web Python de alto nivel que fomenta el rápido desarrollo, un diseño limpio y pragmático, debido a que tiene un núcleo bastante robusto con múltiples librerías que ahorran de manera significativa el trabajo.

“Django fue desarrollado por una operación en línea-noticias, lo cual fue diseñado para manejar dos retos: los plazos intensivos de una sala de redacción y los estrictos requisitos de los desarrolladores web con experiencia que lo escribieron. Permite construir de alto rendimiento, aplicaciones web elegantes rápidamente” [11].

Figura 6. Logo del Framework web Django

5.4. Base de Datos

PostgreSQL es un sistema de gestión de bases de datos objeto-relacional, distribuido bajo licencia de software libre BSD (Berkeley Software Distribution), con menos restricciones, y con su código fuente disponible libremente.

Figura 7. Logo de PostgreSQL

Los ficheros de configuración son tres ficheros principales de configuración que utiliza PostgreSQL los cuales son:

- postgresql.conf,
- pg_hba.conf y
- pg_ident.conf

Dichos archivos de configuración permiten brindar seguridad a Postgres, como bloquear ip's, permitiendo solo las ip's que se haya ingresado, y muchas otras opciones para hacer de la aplicación más segura [12].

5.5. Análisis del sistema

El sistema descrito en este documento es una herramienta didáctica que permite a los usuarios registrarse en el sistema y seguir un curso interactivo en línea orientado a la seguridad en UMTS. Logrando que el aprendizaje de los usuarios sea mediante una herramienta en la que la mayoría pueda acceder y es mediante una página web.

5.6. Requisitos funcionales

- El usuario se podrá registrar en el sistema mediante datos básicos un usuario, correo y una contraseña con la que pueda ingresar al sistema.
- El usuario va a poder elegir libremente los temas a estudiar en la sección de capítulos donde va a encontrar todo el contenido del curso.
- El usuario va a tener la oportunidad de probar sus conocimientos mediante un módulo de lecciones donde se le evaluará, con la finalidad de reforzar su aprendizaje.
- Brindar un módulo donde el usuario tendrá acceso directo a contenido gratuito online donde pueda leer más sobre el tema a tratar.

5.7. Requisitos no funcionales

- La disponibilidad del sistema depende de si el usuario tiene o no conexión a internet.
- El sistema al ser web está orientado a que se puede acceder mediante cualquier dispositivo que cuente con un explorador de internet.
- La disponibilidad del sistema dependería de terceros ya que estaría en un hosting alquilado, y se depende de ese proveedor para la disponibilidad.

5.8. Casos de Uso

En el sistema existen tres tipos de usuarios, el usuario registrado, el usuario sin registrar y el administrador.

El administrador cuenta con las opciones siguientes:

Para el rol de administrador se le permite realizar tareas de mantenimiento de las tablas de la base de datos del sistema, además que el administrador del sistema tiene libre acceso, es decir, también tiene permitido las acciones que tiene el rol estudiante. Las acciones del administrador son:

- Ingresar datos en tablas: El administrador del sistema ingresará los datos básicos para que funcione correctamente la aplicación.
- Editar datos en tablas: Para motivos de mantenimiento existe esta función para que cualquier cambio en el contenido sea fácilmente editado.
- Eliminar datos en tablas: Opción que permite al administrador eliminar datos del sistema.

El usuario registrado cuenta con las siguientes funciones:

- Visitar el sitio: Permite visitar el sitio del sistema web.
- Ingresar al sistema: Permite al usuario ingresar al sistema y poder acceder al contenido en línea.
- Ver Foro: Permite al usuario revisar el foro que se encuentra alojado en el sitio.
- Comentar foro: Permite al usuario comentar cualquier foro que desee.
- Votar por comentarios: Permite al usuario votar por la respuesta más acertada según su criterio en el foro.
- Ver contenido: Se refiere a todo el contenido que pueda acceder desde el sistema.
- Tomar lecciones: Permite al usuario autoevaluarse e ir conociendo como va su avance con lo aprendido en el sistema.

El usuario no registrado cuenta con las siguientes funciones:

- Visitar el sitio: Permite visitar el sitio del sistema web.

- Registrase: Permite al usuario registrarse en el sistema con sus datos.
- Ver Foro: Permite al usuario revisar el foro que se encuentra alojado en el sitio.
- Votar por comentarios: Permite al usuario votar por la respuesta más acertada según su criterio en el foro.
- Ver contenido: Se refiere a todo el contenido que pueda acceder desde el sistema.

5.9. Estructura de la Aplicación Web

LUS está definido bajo la modalidad MVC (modelo, vista, controlador) en Django MVT ("model, view, template", modelo, vista, plantilla), el cual separa los datos y la lógica de negocio de la interfaz de la aplicación y el módulo encargado de gestionar los eventos y las comunicaciones entre los usuarios. Este método es muy efectivo en sistemas de gran tamaño y alcance y mantiene una estructura ordenada de la aplicación.

5.10. Diseño del sistema

El diseño de nuestro sistema está enfocado a ser de fácil uso para el usuario, hemos tomado como referencia algunos sistemas online de cursos para tener una idea más clara de cómo mostrar nuestra idea.

La figura 8 muestra la pantalla principal del sistema, la cual vemos un menú principal, un banner, y un explicativo de lo que hace nuestro pequeño sistema.

Figura 8. Pantalla principal del sistema

En la figura 9 se puede observar algunas opciones como son: inicio, contenido, lecciones, foro, acerca de descritos con más detalle adelante:

En la opción de iniciar sesión es para que los usuarios registrados puedan ingresar al sistema, y así poder acceder a las opciones que son solo para usuarios registrados, las cuales son lecciones, comentar foro y votar en foro.

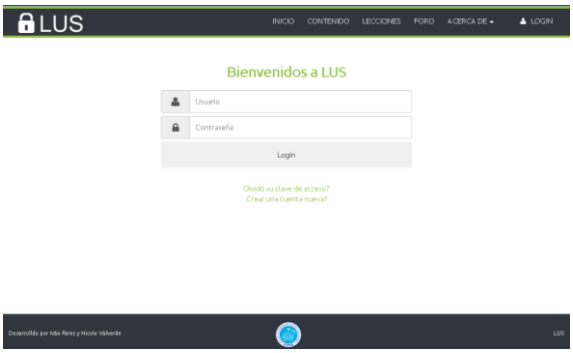

Figura 9. Pantalla de Ingreso al sistema

En la opción de registro, sirve para que los nuevos usuarios se puedan registrar al sistema, llenando un pequeño formulario con datos básicos del usuario, como un nombre, un apellido, sexo, usuario, contraseña y un correo electrónico.

Así quedarán registrados en el sistema y podrán acceder a las opciones de los usuarios registrados.

Figura 10. Pantalla de registro al sistema

La opción de lecciones podrán obtener la lista de las lecciones que tenemos y la podrán tomar todos los usuarios que se encuentren registrados en el sistema.

En la figura 11 se puede observar la lista de las lecciones que tiene el sistema, se puede entrar a cada lección con solo dar clic en la opción "Tomar Lección" en la parte inferior izquierda de cada lección. Esta sección es exclusiva de los usuarios registrados dentro de la plataforma de LUS por medio de su usuario y contraseña previamente creada.

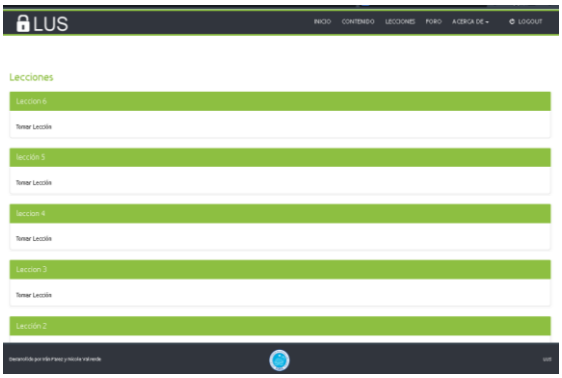

Figura 11. Pantalla de la lista de lecciones

6. Conclusiones

La implementación de un sistema web como herramienta didáctica constituye un aporte para el aprendizaje de los procesos de seguridad en redes 3G como lo es UMTS con toda la información de respaldo que garantiza el acceso a la misma en todo momento.

Redes de tercera generación 3G como UMTS son completamente conmutadas por paquetes para la transferencia de audio y video en tiempo real con modulación WCDMA, para las señales banda base con la finalidad de que se dificulte la intercepción de las señales dispersas en todo el ancho de banda, además que pueda resistir a los ruidos e interferencia del medio.

En la parte de inicialización de alguna sesión, la negociación de los vectores de autenticación realizada entre el AuC y VLR/SGSN es un paso fundamental previo al intercambio de información e inicio de la comunicación entre el usuario (USIM) y el VLR/SGSN, puesto se envían en ellas las funciones criptográficas necesarias para el proceso de verificación, y si es exitosa, las claves generadas CK e IK sean enviadas para así continuar con el procedimiento de proveer integridad y confidencialidad del enlace de tercera generación.

Estos algoritmos, de cifrado por bloques para la integridad f9 y de cifrado de flujo para la confidencialidad f8 son de mucha importancia para la protección de los datos mientras los datos viajan en el enlace entre la red y el usuario evitando suplantación de identidad durante la conexión mediante claves de cifrado que se renuevan en cada proceso de autenticación.

El algoritmo de cifrado KASUMI, base de los algoritmos de confidencialidad f8 y de integridad f9 para proteger las comunicaciones en el intervalo aéreo entre el móvil y la BS. Mientras MILENAGE es un conjunto de algoritmos de autenticación y generación de claves estándar para lograr interoperabilidad segura y confiable entre el AuC con las diferentes implementaciones de la tarjeta SIM.

7. Referencias

[1] Proaño T, Rodríguez E., , «Análisis comparativo del servicio de internet móvil brindado a través de 3G (UMTS) versus la opción brindada por el anexo "e" del estándar IEEE 802.16 (WIMAX MÓVIL),» Escuela Politécnica Nacional, Quito, Ecuador, 2007.

[2] López J., «Simulación de tramas de comunicación para UMTS,» Universidad de las Américas, Puebla, México, 2005.

[3] Heras D., Pauta H., «Estudio del Arte en redes UMTS/3G con el Subsistema IMS,» Universidad Politécnica Salesiana Sede Cuenca, Cuenca, 2011.

[4] Niemi V., Nyberg K., UMTS Security, Finland: John Wiley & Sons, Ltd, 2003.

[5] González A., «Modelos de Seguridad para móviles,» Universidad Carlos III, Madrid, 2010.

[6] Dunkelman O., Keller N:, «An Improved Impossible Differential Attack on MISTY1,» Einsein Institute of Mathematics, Hebrew University, Jerusalem, Israel.

[7] Nyberg K., «Cryptographic Algorithms for UMTS,» ECCOMAS, Jyvaskyla, 2004.

[8] Wallis B., «Hypertext Transfer Protocol (HTTP) Digest Authentication using Global System for Mobile Communications (GSM) A3 and A8,» 4 February 2008. [En línea]. Available: http://tools.ietf.org/html/draft-ietf-http-digest-auth-a3a8-01#page-5.

[9] http://lusonline.net/

[10] González R., Python para todos, España: Creative Commons Reconocimiento 2.5, 2007.

[11] Django Software Foundation, «django,» 2005 - 2014. [En línea]. Available: https://www.djangoproject.com/.

[12] Martinez R., «PostgreSQL-es,» 2009 - 2013. [En línea]. Available: http://www.postgresql.org.es/sobre_postgresql.