



**UNIVERSIDAD ESTATAL DE MILAGRO
FACULTAD CIENCIAS DE LA INGENIERÍA**

**TRABAJO DE TITULACIÓN DE GRADO PREVIO A LA
OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS
COMPUTACIONALES**

**PROPUESTA PRÁCTICA DEL EXAMEN DE GRADO O DE FIN DE
CARRERA (DE CARÁCTER COMPLEXIVO)
INVESTIGACIÓN DOCUMENTAL**

**TEMA: ANÁLISIS DE LA SEGURIDAD DE APLICACIONES
MÓVILES BANCARIAS.**

AUTORES:

**ANDRADE TOSCANO GERARDO DAVID
BRAVO PIÑA JASON ANTONIO**

Acompañante:

**MSC. BRAVO DUARTE FREDDY LENIN
MILAGRO, MAYO DEL 2019
ECUADOR**

DERECHOS DE AUTOR

Ingeniero.

Fabricio Guevara Viejó, PhD.

RECTOR

Universidad Estatal de Milagro

Presente.

Yo, **BRAVO PIÑA JASON ANTONIO** en calidad de autores y titulares de los derechos morales y patrimoniales de la propuesta práctica de la alternativa de Titulación – Examen Complexivo: Investigación Documental, modalidad presencial, mediante el presente documento, libre y voluntariamente procedo a hacer entrega de la Cesión de Derecho del Autor de la propuesta practica realizado como requisito previo para la obtención de mi Título de Grado, como aporte a la Temática **ANÁLISIS DE LA SEGURIDAD DE APLICACIONES MOVILES BANCARIAS** del Grupo de Investigación **PROCESAMIENTO Y ANÁLISIS DE DATOS** de conformidad con el Art. 114 del Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, concedo **a favor de la Universidad Estatal de Milagro una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos. Conservo a mi favor todos los derechos de autor sobre la obra, establecidos en la normativa citada.

Así mismo, autorizo a la Universidad Estatal de Milagro para que realice la digitalización y publicación de esta propuesta practica en el repositorio virtual, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

El autor declara que la obra objeto de la presente autorización es original en su forma de expresión y no infringe el derecho de autor de terceros, asumiendo la responsabilidad por cualquier reclamación que pudiera presentarse por esta causa y liberando a la Universidad de toda responsabilidad.

Milagro, a los 8 días del mes de Mayo del 2019



BRAVO PIÑA JASON ANTONIO

CI: 091913101-1

DERECHOS DE AUTOR

Ingeniero.

Fabricio Guevara Viejó, PhD.

RECTOR

Universidad Estatal de Milagro

Presente.

Yo, **ANDRADE TOSCANO GERARDO DAVID**, en calidad de autores y titulares de los derechos morales y patrimoniales de la propuesta práctica de la alternativa de Titulación – Examen Complexivo: Investigación Documental, modalidad presencial, mediante el presente documento, libre y voluntariamente procedo a hacer entrega de la Cesión de Derecho del Autor de la propuesta practica realizado como requisito previo para la obtención de mi Título de Grado, como aporte a la Temática **ANÁLISIS DE LA SEGURIDAD DE APLICACIONES MOVILES BANCARIAS** del Grupo de Investigación **PROCESAMIENTO Y ANÁLISIS DE DATOS** de conformidad con el Art. 114 del Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, concedo ** a favor de la Universidad Estatal de Milagro una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos. Conservo a mi favor todos los derechos de autor sobre la obra, establecidos en la normativa citada.

Así mismo, autorizo a la Universidad Estatal de Milagro para que realice la digitalización y publicación de esta propuesta practica en el repositorio virtual, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

El autor declara que la obra objeto de la presente autorización es original en su forma de expresión y no infringe el derecho de autor de terceros, asumiendo la responsabilidad por cualquier reclamación que pudiera presentarse por esta causa y liberando a la Universidad de toda responsabilidad.

Milagro, a los 8 días del mes de Mayo del 2019




ANDRADE TOSCANO GERARDO DAVID

CI: 094219290-7

APROBACIÓN DEL TUTOR DE LA INVESTIGACIÓN DOCUMENTAL

Yo, **BRAVO DUARTE FREDDY LENIN** en mi calidad de tutor de la Investigación Documental como Propuesta práctica del Examen de grado o de fin de carrera (de carácter complejo), elaborado por los estudiantes **ANDRADE TOSCANO GERARDO DAVID**, **BRAVO PIÑA JASON ANTONIO** cuyo tema de trabajo de Titulación es **ANÁLISIS DE LA SEGURIDAD DE APLICACIONES MÓVILES BANCARIAS**, que aporta a la Línea de Investigación **PROCESAMIENTO Y ANÁLISIS DE DATOS** previo a la obtención del Grado de **INGENIEROS EN SISTEMAS COMPUTACIONALES**; considero que el mismo reúne los requisitos y méritos necesarios en el campo metodológico y epistemológico, para ser sometido a la evaluación por parte del tribunal calificador que se designe, por lo que lo **APRUEBO**, a fin de que el trabajo sea habilitado para continuar con el proceso de titulación de la alternativa de Examen de grado o de fin de carrera (de carácter complejo) de la Universidad Estatal de Milagro.

En la ciudad de Milagro, a los 8 días del mes de Mayo de 2019.



ING. BRAVO DUARTE FREDDY LENIN, MSC

Tutor

C.I.: 0913170528

APROBACIÓN DEL TRIBUNAL CALIFICADOR

El tribunal calificador constituido por:

FREDDY LENIN BRAVO DUARTE

MIRELLA AZUCENA CORREA PERALTA

LUIS CRISTOBAL CORDOVA MARTINEZ

Luego de realizar la revisión de la Investigación Documental como propuesta práctica, previo a la obtención del título (o grado académico) de **INGENIERA EN SISTEMAS COMPUTACIONALES** presentado por el señor **BRAVO PIÑA JASON ANTONIO**.

Con el tema de trabajo de Titulación: **ANÁLISIS DE LA SEGURIDAD DE APLICACIONES MÓVILES BANCARIAS**.



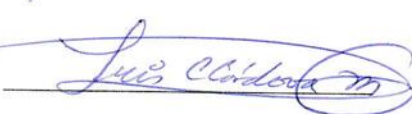
Otorga a la presente Investigación Documental como propuesta práctica, las siguientes calificaciones:

Investigación documental	[78,67]
Defensa oral	[14,33]
Total	[93]

Emite el siguiente veredicto: (aprobado/reprobado) APROBADO

Fecha: 08 de Mayo del 2019.

Para constancia de lo actuado firman:

	Nombres y Apellidos	Firma
Presidente	FREDDY LENIN BRAVO DUARTE	
Secretario /a	MIRELLA AZUCENA CORREA PERALTA	
Integrante	LUIS CRISTOBAL CORDOVA MARTINEZ	

APROBACIÓN DEL TRIBUNAL CALIFICADOR

El tribunal calificador constituido por:

FREDDY LENIN BRAVO DUARTE

MIRELLA AZUCENA CORREA PERALTA

LUIS CRISTOBAL CORDOVA MARTINEZ

Luego de realizar la revisión de la Investigación Documental como propuesta práctica, previo a la obtención del título (o grado académico) de **INGENIERA EN SISTEMAS COMPUTACIONALES** presentado por el señor **ANDRADE TOSCANO GERARDO DAVID**.

Con el tema de trabajo de Titulación: **ANÁLISIS DE LA SEGURIDAD DE APLICACIONES MÓVILES BANCARIAS**.




Otorga a la presente Investigación Documental como propuesta práctica, las siguientes calificaciones:

Investigación documental	[79]
Defensa oral	[16]
Total	[95]

Emite el siguiente veredicto: (aprobado/reprobado) APROBADO

Fecha: 08 de Mayo del 2019.

Para constancia de lo actuado firman:

	Nombres y Apellidos	Firma
Presidente	FREDDY LENIN BRAVO DUARTE	
Secretario /a	MIRELLA AZUCENA CORREA PERALTA	
Integrante	LUIS CRISTOBAL CORDOVA MARTINEZ	

DEDICATORIA

Quiero expresar mi gratitud a Dios por haberme dado la vida y permitirme el haber llegado hasta este momento tan importante de mi formación profesional.

A mis padres Luis Alberto Bravo y Dora Piña quienes con su amor, paciencia y esfuerzo me han permitido llegar a cumplir hoy un sueño más, gracias por inculcar en mí el ejemplo de esfuerzo y valentía, de no temer las adversidades porque Dios está conmigo siempre.

A mis hermanos Luis Bravo, Steve Bravo, Ronald Bravo por su cariño y apoyo incondicional, durante todo este proceso, por estar conmigo en todo momento gracias.

A mi familia que siempre me brinda consejos y palabras de aliento hicieron de mí una mejor persona y de una u otra forma me acompañan en todos mis sueños y metas.

A mis amigos por apoyarme cuando más los necesité estaban ahí, por extender su mano en momentos difíciles y por el amor brindado cada día, de verdad mil gracias, siempre los llevo presente.

Jason Antonio Bravo Piña

Al creador de todas las cosas, al que escucha mis oraciones y me da fuerzas para continuar y levantarme cuando a punto de caer he estado; por ello, con toda la humildad que de mi corazón puede emanar, dedico primeramente mi trabajo a Dios.

A mis padres Freddy y Eulalia por su apoyo constante, por llenar mi vida con sus valiosos consejos y valores. Por ser mi mayor inspiración y quienes con su amor, paciencia y confianza me han permitido lograr mi meta más anhelada.

A mi hermana Adriana por ser el ejemplo de una hermana mayor de la cual aprendí que la vida no es fácil y que todo esfuerzo tiene su recompensa. A mi hermano Oscar que siempre ha estado junto a mí, por su cariño y apoyo incondicional.

A mis abuelitos Luis y Mercedes por quererme y apoyarme siempre. Por ser mis consejeros y ejemplos a seguir, esto también se lo debo a ustedes.

Gerardo David Andrade Toscano

AGRADECIMIENTO

Agradezco a Dios por protegerme durante todo el camino que he recorrido y darme muchas fuerzas para superar muchos obstáculos y barreras a lo largo de mi vida. A mi familia por ser mi motor, mi inspiración, por los valores que me enseñaron a lo largo de mi vida. A todas las personas que confiaron en mí y me brindaron su apoyo desinteresadamente cuando más los necesité. A todos los docentes que me inculcaron sus conocimientos, su experiencia y trabajo. A mi Tutor el Ing. Bravo Duarte Freddy Lenin, por brindarme sus conocimientos y el apoyo a lo largo de la elaboración del proyecto de titulación.

Jason Antonio Bravo Piña

Agradezco a Dios ya que sin él sería imposible dar este paso tan importante en mi vida, por darme las fuerzas necesarias en los momentos en que más las necesité y bendecirme siempre en todo momento y tener la oportunidad de caminar a su lado por el resto de mi vida.

A mis padres que siempre estuvieron en los momentos más difíciles, gracias por apoyarme en todo momento y darme esas palabras que tanto las necesite, esto es por ustedes y para ustedes para que una vez más se sienta orgullosos de mi por escalar un peldaño más en mi vida profesional.

A mis queridos hermanos por siempre estar conmigo y no dejar que me derrumbara por nada, a toda mi familia en general, a mis amigos que de una u otra manera siempre estuvieron ahí para darme las fuerzas necesarias, ese empuje y motivación para seguir adelante y cumplir este sueño.

Agradezco a nuestros docentes en general y de manera especial a nuestro tutor Ing. Freddy Bravo quien con su conocimiento y experiencia nos ha guiado en la elaboración de este proyecto.

Gerardo David Andrade Toscano

ÍNDICE GENERAL

DERECHOS DE AUTOR	I
DERECHOS DE AUTOR	II
APROBACIÓN DEL TUTOR DE LA INVESTIGACIÓN DOCUMENTAL	III
APROBACIÓN DEL TRIBUNAL CALIFICADOR	IV
APROBACIÓN DEL TRIBUNAL CALIFICADOR	V
DEDICATORIA	VI
AGRADECIMIENTO	VII
ÍNDICE GENERAL	VIII
ÍNDICE DE FIGURAS	X
ÍNDICE DE TABLAS	XI
RESUMEN	1
ABSTRACT	1
INTRODUCCIÓN	3
CAPÍTULO 1	4
1.1 Planteamiento del problema	4
1.2 Objetivo General	5
1.3 Objetivos Específicos	5
1.4 Justificación	5
CAPÍTULO 2	6
MARCO TEÓRICO CONCEPTUAL	6
2.1 Seguridad de Sistemas (Aplicaciones)	6
2.2 Autenticación y Autorización:	6
2.3 Bases sobre la Seguridad de Software	6
2.3.1 Política default a prueba de errores:	7
2.3.2 Mediación completa:	7
2.3.3 División de privilegios:	7
2.3.4 Modelo abierto:	7
2.3.5 Privilegios mínimos de software:	7
2.3.6 Métodos menos comunes:	7
2.3.7 Economía de mecanismos:	7
2.4 Desarrollo de Apps móviles.	7

2.4.1 Apps Web móviles:	8
2.4.2 Apps Nativas:	8
2.4.3 Apps web embebidas:	8
2.5 Privacidad de datos personales y del dispositivo móvil.	9
2.6 La Plataforma del desarrollo Android	9
2.7 Arquitectura Android.....	9
2.8 Reserva y Seguridad de Android.....	11
CAPÍTULO 3	14
METODOLOGÍA	14
3.1 Puntos vulnerables a examinar	15
3.2 Aplicación de la Ingeniería Inversa y medio de transporte (Análisis)	15
3.3 Analizador Wireshark:	16
3.4 Plugin FindBugs:	16
CAPÍTULO 4	18
DESARROLLO DEL TEMA	18
4.1 Análisis de Seguridad en el Transporte de Envío de Datos	20
4.2 Análisis del comportamiento de las aplicaciones	21
4.2.1 Vulnerabilidades a encontrar	22
4.3 Análisis de tráfico procedente del aplicativo móvil del Banco del Pacifico.	23
4.4 Análisis de tráfico procedente del aplicativo móvil del Banco de Guayaquil.	26
4.5 Análisis estático del aplicativo (APK).....	30
4.5.1 Vulnerabilidades a encontrar	30
CAPÍTULO 5	42
CONCLUSIONES.....	42
REFERENCIAS BIBLIOGRÁFICAS.....	43
Bibliografía	43

ÍNDICE DE FIGURAS

Figura 1 Arquitectura S.O Android	10
Figura 2 Requerimiento de permisos Android.....	11
Figura 3 Uso proxy prueba para verificar conexión entre el cliente y el servidor	21
Figura 4 Configuración para el análisis.....	22
Figura 5 Seleccionamos interfaz a filtrar (WIFI).....	23
Figura 6 Ping hacia el dominio Banca Móvil Pacifico.....	24
Figura 7 Se añade filtro de dirección IP	24
Figura 8 Resultados obtenidos con el filtro añadido	25
Figura 9 Error de respuesta: Segmento no capturado	25
Figura 10 Error de retransmisión Aplicativo Móvil Pacifico	26
Figura 11 Seleccionamos interfaz a filtrar (WIFI).....	26
Figura 12 Ping hacia el dominio Banca Móvil Guayaquil	27
Figura 13 Filtro con dirección IP publica de la banca móvil.....	27
Figura 14 Tráfico generado por parte de la banca Móvil	28
Figura 15 Análisis de resultados por protocolo ICMP	29
Figura 16 Descargas de los APK de los aplicativos.....	31
Figura 17 Eclipse y su plugin FindBugs	31
Figura 18 Archivo con información base del aplicativo	32
Figura 19 Configuración en el proyecto del aplicativo	32
Figura 20 Creamos un proyecto base	33
Figura 21 Copiamos el APK a la raíz del proyecto.....	33
Figura 22 Aplicamos el plugin	34
Figura 23 Abrimos el archivo con bugs encontrados.....	35
Figura 25 Resultados App Banco Pichincha	36
Figura 26 Resultados App Banco Produbanco	36
Figura 28 Otros parámetros arrojados	37
Figura 29 Resultado App Banco Internacional.....	38
Figura 30 Resultados App Banco de Loja.....	39
Figura 31 Resultado App Banco Bolivariano	40
Figura 32 Resultado Banco de Pacifico	40
Figura 33 Resultados App Banco Guayaquil	41

ÍNDICE DE TABLAS

Tabla 1 Aplicaciones Móviles a estudiar.	14
Tabla 2 Permisos de las Apps para Android en sus versiones posteriores.	18

TEMA: “ANALISIS DE LA SEGURIDAD DE APLICACIONES MÓVILES BANCARIAS”.

RESUMEN

En la actualidad muchas de las entidades u organizaciones financieras en el Ecuador ofrecen día a día una mejor forma de operar con sus clientes de manera directa, esto lo realizan mediante la llamada Banca Móvil o Banca Virtual. Básicamente el cliente final procede a descargar una aplicación a su dispositivo móvil; la misma le permite generar operaciones bancarias muy básicas entre las cuales tenemos: Consulta de saldo, ver últimos movimientos, cambio de datos personales, verificar el estado de la información de su tarjeta de crédito o débito o incluso realizar transferencias de dinero entre distintas entidades bancarias, consultar así mismo la ubicación de los cajeros automáticos más cercanos a través del uso del Google Maps. Dado a que estas App hacen uso de información muy delicada de los clientes como es la información personal, geográfica e incluso información financiera surge la duda y la pregunta ¿Cuál es el grado de seguridad que nos proporcionan estas entidades en base a nuestra integridad? Para poder solucionar o dar respuesta a esta pregunta se analizarán varias aplicaciones bancarias desarrolladas en el sistema operativo Android, las cual podemos encontrarlas en la tienda de Google. Cada aplicación se analizará minuciosamente mediante el uso de la ingeniería inversa, analizar parte del APK y el método aplicado para él envío de datos desde el cliente hacia el servidor.

Otro de los objetivos de este documento es clasificar las aplicaciones ofrecidas por las entidades bancarias y dar lineamientos en base a las buenas prácticas de seguridad al momento de generar una aplicación y ponerla en funcionamiento para los clientes.

PALABRAS CLAVE: aplicaciones bancarias, banca virtual, seguridad móvil.

ABSTRACT

At present, many of the entities or financial organizations in Ecuador offer a better way to operate with their clients every day in a more direct way, this is done through the so-called Mobile Banking or Virtual Banking. Basically the final client proceeds to download an APP to your mobile device, which allows you to generate very basic banking operations, among which we have: Balance inquiry, view latest movements, change personal data. Check the status of your credit or debit card information or even make money transfers between different banks, also check the location of the nearest ATMs through the use of Google Maps. Given that these App make use of very sensitive information from customers such as personal information, geographical and even financial information the question arises and the question: What is the degree of security that these entities provide us based on our integrity? In order to solve or answer this question, we will analyze several banking applications developed in the Android operating system, which can be found in the Google store. Each application will be thoroughly analyzed through the use of reverse engineering, analyze part of the source code and see the kind of method applied to send data from the client to the server.

Another objective of this document is to classify the banking applications offered by banking entities within the taxonomy and to give guidelines based on good security practices when generating an application and putting it into operation for clients.

KEY WORDS: banking applications, virtual banking, mobile security.

INTRODUCCIÓN

Mediante el pasar de los años, las entidades financieras han publicado al mercado aplicaciones que dan la facilidad de interactuar al cliente con el banco de una forma más fácil y desde la comodidad de su hogar, haciendo uso de sus dispositivos móviles. Estos lanzamientos vienen enganchados de fuertes campañas publicitarias. Sin embargo, de ahí surge la duda ¿Es la seguridad un factor importante en el desarrollo de estas aplicaciones bancarias? Mucho de los clientes no tiene ni la más remota idea ni interés sobre el uso que le dan estas entidades a su información personal; sin embargo, hay otras que no. A eso se añaden los riesgos asociados al desarrollo de aplicaciones móviles, los cuales de no ser controlados podrían significar que sus usuarios sean víctimas de ataques a la confidencialidad de su información y puedan ser extorsionados e incluso víctimas de fraudes informáticos. La información que debe ser protegida en los dispositivos móviles básicamente forma parte de estas tres clases: Información Bancaria: Dinero almacenado en la cuenta del usuario, transacciones que realizan los clientes, número de las tarjetas de crédito o débito y su password, etc. Información Personal: Datos personales del cliente (nombre, apellido, dirección, email, números telefónicos, etc.), geográficos (ubicación del cliente y puntos guardados), fotos, archivos descargados, etc. Información del aparato: Identificadores del dispositivo móvil (IMSI, IMEI, ANDROID_ID).

Por este motivo es de vital importancia poder estudiar la seguridad de las aplicaciones lanzadas al mercado por el lado de las entidades financieras, ya que las consecuencias de un ataque pueden ser las siguientes: Fallo en medio proceso de generar alguna transacción, filtrado de datos principales del cliente mediante el uso de herramientas fraudulentas, robo de credenciales de autenticación (ej. Usuario / Contraseña) del usuario; las mismas podrían ser reutilizadas por los atacantes para acceder a su información bancaria; o peor aún, realizar transacciones monetarias a otras cuentas mediante el uso de su propia cuenta.

CAPÍTULO 1

PROBLEMA DE INVESTIGACIÓN

1.1 Planteamiento del problema

Gran cantidad de usuarios en la actualidad hacen uso de la Banca Virtual ya sea para realizar consultas básicas o realizar transacciones.

Mucha de estas entidades ofrece amplia información al cliente para que el mismo esté al tanto de su estado de cuenta, todo esto se lo lleva mediante procesos informáticos en los cuales tanto como la entidad y el usuario final interactúan en tiempo real. En términos informáticos a este tipo de interacción se la denomina comunicación cliente/servidor, básicamente consiste en un servidor que responde peticiones en base a pedidos por parte del cliente final, al ser un medio de comunicación bastante usado por parte de los desarrolladores de aplicaciones móvil ya sean bancarias o de otro fin, al existir gran cantidad de tráfico es propensa a ser atacada o a sufrir fallos durante la ejecución de una transacción o de una petición en general.

Parte de los desarrollares o grupo de desarrollo en estas entidades bancarias, en la actualidad hacen usos de certificados poco obsoletos como: El certificado SSL/TLS, él mismo debe ser manipulado de forma adecuada, debe ser firmado en base a un algoritmo seguro o fuerte (ASHA2), la cadena de conexión debe estar parametrizada de forma correcta para garantizar el no permitir un bypass en la autenticación correspondiente; sin embargo no muchas veces se lo realiza de esta forma, lo que provoca que haya conflictos al realizar una sesión o una transacción en las aplicaciones.

“Evaluar la seguridad que nos proporciona el desarrollo de estas aplicaciones en la plataforma Android en el contexto pleno de la seguridad, en aspectos primordiales como herramientas disponibles en su API, su base root al acceso a los recursos, riesgos asociados a su fragmentación, el mal uso de estos recursos, así como el mal desarrollo de estas aplicaciones es un factor clave”. (Cabello, 2015)

1.2 Objetivo General

- Evaluar las aplicaciones bancarias basadas en la plataforma Android en el contexto de seguridad, en puntos como: herramientas para elaboración de la aplicación, privilegios y permisos al usuario.

1.3 Objetivos Específicos

- Elaborar una serie de procedimientos para verificar si es posible tener falencias (hacer uso de plugin en plataformas de desarrollo Android) en la aplicación.
- Realizar una comparación del grado de seguridad con la que constan varias de las entidades financieras a estudiar.
- Utilizar un proxy para medir el grado de seguridad y comunicación que hay con el servidor final, a su vez escuchar el tráfico que se genera en toda una red y realizar filtros de búsqueda.

1.4 Justificación

Desde un enfoque conceptual, la seguridad de las aplicaciones bancarias es importante en cualquier aspecto, la misma esta propensa a ser vulnerada por parte de terceros al tratar de generar alguna petición a los servidores bancarios.

Por otra parte, existen en el mundo de desarrollo de aplicaciones móviles varios aplicativos, herramientas y plugin los cuales dan acceso a información clave (APK) de estas aplicaciones bancarias y pueden ser manipuladas ya sea para bien o mal.

Podemos notar que las aplicaciones móviles ayudan al cliente a tener una mejor manipulación o entendimiento de procedimientos o procesos informáticos por medio de una interfaz de usuario muchas veces amigable, la misma permite crear una comunicación, cliente - aplicativo – servidor remoto.

CAPÍTULO 2

MARCO TEÓRICO CONCEPTUAL

2.1 Seguridad de Sistemas (Aplicaciones)

El grado de seguridad de un sistema o software de información está identificado como la capacidad que tiene el mismo para funcionar de forma normal o adecuada, aun estando dentro de un entorno hostil. Si hablamos de forma más específica de seguridad de sistema, está definida como la elaboración del sistema que sea capaz de funcionar de forma correcta aun siendo atacado por programas maliciosos. (Hevia, 2009)

Existen dos definiciones que sirven como base para llevar un análisis de seguridad de un sistema, los cuales son:

La Autenticación y Autorización.

2.2 Autenticación y Autorización:

Este proceso es llevado a cabo mediante la identificación, el software pregunta al usuario final por algún tipo de objeto o elemento el cual le permita identificar si realmente es el usuario indicado o no.

Mediante la autenticación, el software valida los datos del LOGIN presentadas por el usuario en la etapa de identificación para verificar si es el indicado o no.

Una vez que se realizan los dos procesos anteriores, el software procede a verificar privilegios y da acceso al usuario, a este proceso se le determina autorización.

2.3 Bases sobre la Seguridad de Software

En inicio de los años 1970, Schroeder y Saltzes hacen público la primera información sobre seguridad en la información de software. En su publicación ellos dan definiciones sobre siete bases de la seguridad de la información. (Robles, 2015)

A continuación, se definen cada una de ellas:

2.3.1 Política default a prueba de errores: Esta política es aquella que se define como base para la elaboración de cualquier software de información.

2.3.2 Mediación completa: Aquí se define que una vez que un individuo o usuario del sistema tenga la necesidad de ingresar al sistema, los permisos de cada sujeto sobre el objeto deben estar previamente identificados para su posterior ingreso.

2.3.3 División de privilegios: El grado de seguridad de un software es blindado mediante la división de múltiples actores para poder realizar acciones de riesgo sobre el sistema.

2.3.4 Modelo abierto: El modelo de estos sistemas no pueden depender de secretos o componentes ocultos para reforzar la seguridad ya que esto podría ocasionar niveles aún más bajos de seguridad a través de la oscuridad de los componentes.

2.3.5 Privilegios mínimos de software: Este punto hace referencia a los módulos con los que el cliente puede interactuar en la aplicación, permisos mínimos al realizar su labor y nada más.

2.3.6 Métodos menos comunes: Esta función considera que deben ser reducidos los mecanismos comunes entre los diversos sujetos con diferentes niveles de privilegios a diversos grupos de sujetos; se los agrupa según su privilegio.

2.3.7 Economía de mecanismos: Estos software deben ser mantenidos lo más simple posible de forma que no sea confuso para el usuario final, ya que la revisión y corrección de código fuente no sean tan vulnerables y así estos se tornen más complejos para ser ultrajados.

2.4 Desarrollo de Apps móviles.

La elaboración de App móviles es diversa al desarrollo de las mismas para equipos de escritorio o dispositivos móviles. Empezando de la forma de manipulación o interacción que existen entre estos dos tipos de dispositivos. Como ya tenemos conocimiento en los dispositivos móviles no es necesario hacer uso de una pantalla para visualizar la información, tampoco el teclado para el ingreso de datos o para apuntar la información que necesitamos. (Cabello, 2015)

Otro principio importante que marca diferencia a los dispositivos móviles de los equipos de escritorio o convencionales son los recursos con los que consta cada uno de estos, cada uno cuenta con sus distintos recursos como, por ejemplo:

En el pc de escritorio o dispositivo de escritorio contamos con un disco duro, internet periférico de e/s bluetooth, mientras que en el caso de los dispositivos móviles tenemos el GPS para la ubicación en tiempo real, lista de direcciones, lista de llamadas, SMS, brújula, sensores entre variedades de recursos.

Clasificación y estudio de las aplicaciones móviles:

2.4.1 Apps Web móviles: Básicamente son desarrolladas con el propósito de evolucionar la aplicación; esto se lo lleva gracias al desarrollo de nuevas versiones entre la aplicación, así como también tratar de hacer uso de la menor cantidad de recursos, hacer uso de la combinación entre CSS Y HTML, uso de JavaScript entre otras API para el desarrollo.

2.4.2 Apps Nativas: Son aplicaciones las cuales son desarrolladas para el propio sistema operativo en el cual está funcionando; hacen uso de funciones provistas, las API'S incorporadas en el propio dispositivo de cada plataforma.

2.4.3 Apps web embebidas: Esta es una mezcla entre una aplicación web y una aplicación nativa, se lo puede llevar a cabo mediante el uso del WebView, este permite incrustar un browser dentro de una aplicación nativa, esta aplicación permite al usuario final interactuar con el sitio web móvil.

2.5 Privacidad de datos personales y del dispositivo móvil.

Hoy en día es mucho más accesible la penetración de la computación móvil, ya que manejamos variedad de información web en nuestros dispositivos, datos como: información personal, fotos, mensajes, registro de llamada, ubicación, entre otra variedad de información. Existe una definición sobre el contenido que dejamos en el sitio que visitamos en redes inalámbricas el cual se define como Traza digital, esta permite a las organizaciones poder elaborar una aplicación haciendo uso del profiling mediante el marketing acerca de nosotros. (Cambria, 2013). Haciendo uso de esta herramienta pueden acceder a nuestros datos personales incluso datos de ubicación en tiempo real.

Otra forma de obtener nuestra información es haciendo el uso de cruce de información, mediante la obtención de datos haciendo relación entre múltiples bases de datos, estas se relacionan mediante uno o más datos comunes en estos registros. Los registros son utilizados

para el linkability para identificar el RUT de una persona, su IMEI del móvil, correo electrónico o credenciales de ingreso.

2.6 La Plataforma del desarrollo Android

Esta es una empresa que forma parte de Google en 2005, dos años posteriores se crea Open Hantset, la misma tiene como objetivo crear un sistema operativo libre o de código abierto para estos dispositivos y tuvo su primer lanzamiento en el año 2008 en el dispositivo móvil T-MOBILE G1.

Versiones: Esta plataforma ha tenido grandes y variadas versiones en su vida hasta poder convertirse en la numero uno para los Smartphone, incluso Tablet, reloj y recientemente los automóviles y los televisores. Es curioso saber que cada una de las versiones está basadas en algún dulce, fecha de lanzamiento y versión a nivel de API.

Cabe mencionar que un sistema operativo de código abierto es propenso a ser tomado por parte de los desarrolladores, los cuales pueden desarrollar nuevas versiones o versiones alternativas como *Cyanogenmod*; la cual oficialmente no forma parte del equipo de Android, pero aporta de forma externa al desarrollo del mismo.

Kernel: Está basado en Linux 2.6 parchado de forma tal que pueda funcionar en distintos teléfonos. Este Kernel hace uso de variedades de drivers que permiten el uso de diferentes componentes del teléfono, así como cámara, bluetooth GPS entre otros componentes que actúan como una capa de abstracción entre el software y el hardware y las demás capas.

2.7 Arquitectura Android

La plataforma Android está compuesta por un conjunto de capas el cual está basada en una pila, mediante la misma se da acceso a que las aplicaciones tengan provecho al cien por ciento de los recursos del dispositivo final.

A continuación, se muestra en la figura 1 la arquitectura de Android.

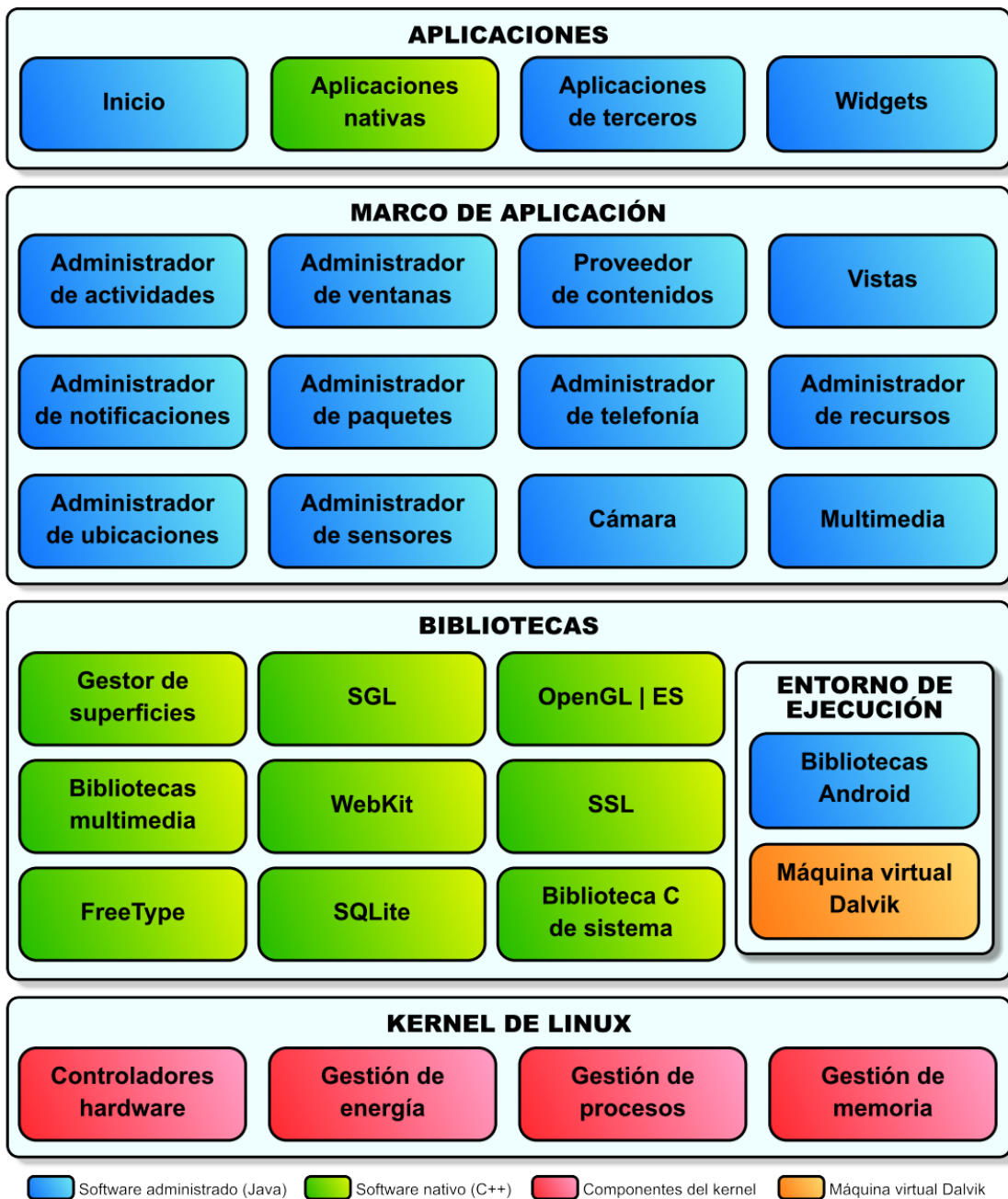


Figura 1. Arquitectura S.O Android

Fuente: Elaboración propia

Biblioteca: El sistema operativo está compuesta por un conjunto de bibliotecas que dan acceso al manejo de cada uno de sus módulos, estas son específicas en base a cada hardware incluido en el móvil.

Entre las bibliotecas a destacar en el sistema operativo tenemos Media Framework el cual permiten dar ejecución a información multimedia como audio o video. Una de las primordiales bibliotecas es SQLite el cual permite gestionar y almacenar información en la base de datos del sistema operativo. La biblioteca OPENGL da acceso a creación de gráficos en 2 o 3D.

2.8 Reserva y Seguridad de Android

El apartado de seguridad en la plataforma Android está basada en una entidad de acceso DAC, el mismo se caracteriza por su modelo de permisos y su sistema aislado (Sandbox). Al momento de ser instalada una aplicación en el sistema, esta es aislada usando funciones propias del Kernel del sistema ya que cada una de las aplicaciones constan de un usuario Linux, lo cual indica que sus datos sean accesibles por una sola aplicación generando que no haya acceso por parte de otras aplicaciones a sus datos.

En la figura 2 podemos observar el requerimiento de permisos al momento de instalar una aplicación en el sistema.

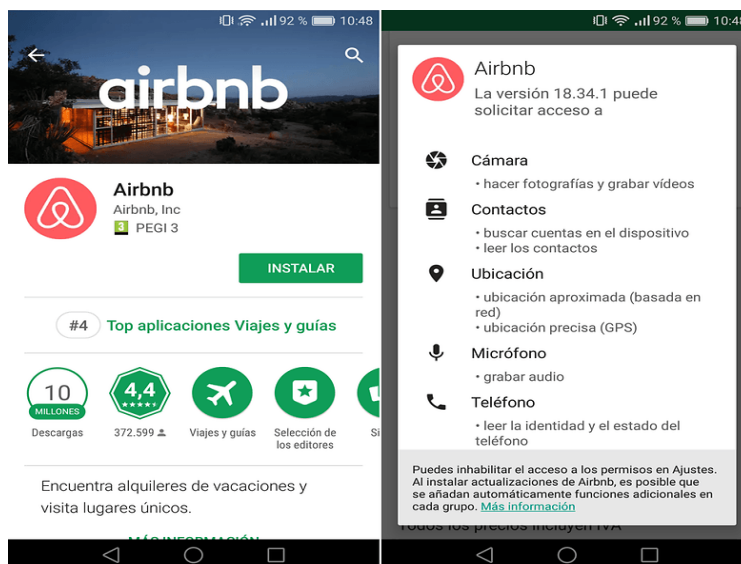


Figura 2. Requerimiento de permisos Android

Fuente: Elaboración propia

2.9 Segmentación

Android es una plataforma de código abierto, la cual permite que cualquier desarrollador o proveedor de hardware pueda implementar nuevos dispositivos o componente basados en su plataforma, con sus propias funcionalidades añadiendo características propias; esto genera un fenómeno el cual se lo denomina como segmentación, el cual da a entender que Android no es una plataforma estandarizada; al contrario permite múltiples configuraciones en sus componentes en los siguientes aspectos del dispositivo móvil.

- Versión del S.O y API
- Aplicaciones extras añadidas externamente
- Sensores (Biométrico, móvil, temperatura, GPS).
- Capacidad de almacenamiento
- Resolución de pantalla
- Marcas de proveedor Hardware

2.10 Aplicaciones dañinas – Instalación

La empresa Google básicamente ofrece a los desarrolladores y a los usuarios finales la plataforma Play Store, esta permite la distribución de aplicaciones para la plataforma. Si bien esta aplicación permite una adecuada distribución y clasificación de las aplicaciones, esta también da el acceso al creador a elaborar aplicaciones malware interna o externamente.

Así como Google nos permite instalar aplicaciones provenientes de la Play Store, esta también da acceso al usuario a instalar aplicaciones de fuentes externas o fuentes desconocidas como lo denomina el sistema operativo Android.

Si el usuario permite o da acceso a la instalación de una aplicación externa o de fuente desconocida el equipo advertirá al usuario de tal acción como un riesgo para el equipo.

Esta advertencia tiene un propósito: al no existir un control sobre esta aplicación el usuario es propenso a sufrir riesgos en su información personal, lo cual causa los siguientes efectos en el dispositivo.

- Filtrado de imágenes y multimedia
- Generación automática de llamadas o envío SMS
- Envío de spam vía Mail o SMS
- Cambios en la configuración interna
- Robo de información o secuestro de teléfonos.

CAPÍTULO 3

METODOLOGÍA

Para identificar los riesgos que pueden tener las App bancarias en el Ecuador que están alojadas en la tienda Play Store, hemos seleccionado y clasificado estas App de la siguiente manera:

Las aplicaciones deben ser nativas del país residente (Ecuador).

Las aplicaciones deben estar alojadas en la tienda Google Play Store, en la tabla 1 podemos observar las aplicaciones web móviles a analizar.

Tabla 1 Aplicaciones Móviles a estudiar.

Aplicación Web	Versión Android	¿Qué página utiliza para acceder a la cuenta bancaria en PC?	¿Utilizan sistema biométrico?
Banca Móvil (Banco Bolivariano).	Android 4.4	24 online	NO
Citi Private Bank In View.	Android 1.7.1	CitiDirect	SI
Amazonas Móvil by Banco Amazonas S.A.	Android 1.4.1	https://www4.bancoamazonas.com/	NO
Banca MOVIL (Banco Guayaquil).	Android 4.4	https://www.bancoguayaquil.com	SI
Banco de Loja S. A	Android 1.0.2	https://www.bancodeloja.fin.ec	NO
Banco Produbanco S.A	Android 2.6.2	https://www.produbanco.com.ec	NO
Banco del Pacifico S.A	Android 4.1	https://www.bancodelpacifico.com/	SI
Banco Internacional S.A	Android 1.42	http://www.finca.ec	NO
Banco del Pichincha S.A	Android 5.3	https://www.pichincha.com	SI

Nota: App Bancarias (elaboración propia)

Cabe mencionar que para este proyecto se seleccionó un conglomerado del total de aplicaciones móviles habilitadas en la Google Play.

3.1 Puntos vulnerables a examinar

Framework embebidos en las aplicaciones los cuales contengan vulnerabilidad cubiertas en su base de datos con software CVE.

Uso de texto plano como envío de transporte, en caso de que la aplicación haga uso de HTTP para realizar algún tipo de petición a los servidores para el envío y recepción de datos. (H. K. Ham, 2011)

- Uso de protocolos ya no hábiles como el SSL en su versión 2 y su versión 3.
- Uso de algoritmos obsoletos como DES, REC4.
- Error en configuración con servidor.
- Tipo de conexión con la base de datos: es importante para visualizar servicios web pesados (WDSL, XML) y livianos como (REST-JSON).
- Información sensible almacenada en el propio dispositivo: login para ingreso a la aplicación, cookies de identificación, archivos de configuración o transacción.
- Permisos con grado alto de riesgo: un ejemplo es acceso a contactos, escritura o edición de archivos fuera del área de almacenamiento, visualización de log o registro de la aplicación.

3.2 Aplicación de la Ingeniería Inversa y medio de transporte (Análisis)

Cabe recalcar que las aplicaciones desarrolladas en Android están compuestas de un archivo APK, el mismo contiene los siguientes puntos:

- **Manifest:** O también llamado manifiesto de la aplicación; este es un archivo XML el cual declara la clase principal, los permisos que se requieren, componentes claves de servicio, el mínimo nivel de la API que debe contener para que se pueda ejecutar, bibliotecas internas y externas para el funcionamiento.
- **Recursos:** Hardware y software necesario para su ejecución, archivos de tipo de letra, archivos de imágenes y múltiples idiomas.
- **Bibliotecas necesarias:** En este archivo se almacenan bibliotecas nativas para el funcionamiento, cada una de estas se basa en su plataforma, la cual puede ser ARM, x86, x64, dependiente del requerimiento de la aplicación.

Como objetivo tenemos la obtención del APK del aplicativo bancario, extrayendo el mismo desde un archivo JavaScript almacenado dentro de su directorio raíz; esto se lo lleva a cabo mediante el uso de un proceso clave llamado de compilación o extracción.

Mediante el uso de la aplicación *Sebar* se logra realizar este procedimiento, esta aplicación está compuesta de un conjunto de herramientas que se las usan para hacer ingeniería inversa en las App móviles. (Díaz, 2015)

3.3 Analizador Wireshark:

Es un analizador de protocolos que actualmente está disponible para plataformas Windows y Unix. Su principal objetivo es el análisis de tráfico, pero además es una excelente aplicación didáctica para el estudio de las comunicaciones y para la resolución de problemas de red. Wireshark implementa una amplia gama de filtros que facilitan la definición de criterios de búsqueda para los más de 1100 protocolos soportados actualmente y todo ello por medio de una interfaz sencilla e intuitiva que permite desglosar por capas cada uno de los paquetes capturados

3.4 Plugin FindBugs:

FindBugs es una herramienta de código abierto que se utiliza para realizar análisis estáticos en código Java para identificar posibles errores de software. Findbugs proporciona comentarios tempranos sobre posibles errores en el código. Esto ayuda al desarrollador a acceder a estos problemas al principio de la fase de desarrollo.

El análisis de Findbugs se puede integrar en los IDE existentes, como el IDE de Eclipse.

Puede deseleccionar libremente las categorías no deseadas, elevar el rango mínimo para informar, especificar la confianza mínima para informar y personalizar los marcadores para los rangos de errores: Advertencia, Información o Error.

FindBugs divide defectos en muchas categorías:

- **Corrección:** recopila errores generales, por ejemplo, bucles infinitos, uso inapropiado, etc.
- **Mala práctica,** por ejemplo, manejo de excepciones, flujos abiertos, comparación de cadenas, etc.

- **Rendimiento**, por ejemplo, objetos inactivos
- **Corrección** de subprocesos múltiples: reúne inconsistencias de sincronización y varios problemas en un entorno de subprocesos múltiples
- **Vulnerabilidad de código malicioso**: reúne vulnerabilidades en el código, por ejemplo, fragmentos de código que pueden ser explotados por posibles atacantes.
- **Seguridad**: reúne agujeros de seguridad relacionados con protocolos específicos o inyecciones de SQL.
- **Dodgy**: recopila olores de código, por ejemplo, comparaciones inútiles, comprobaciones nulas, variables no utilizadas, etc.

CAPÍTULO 4

DESARROLLO DEL TEMA

Tabla 2 Permisos de las Apps para Android en sus versiones posteriores.

Aplicación Web	Versión Android	Permisos para la Aplicaciones
Banca Móvil (Banco Bolivariano).	Android 4.4	Cámara(<i>realizar fotografías y videos</i>), Contactos(<i>consultar tus contactos</i>), Ubicación(<i>acceder a tu ubicación aproximada</i>), Teléfono (<i>consultar la identidad y el estado del teléfono</i>), Almacenamiento (<i>modificar o eliminar contenido de la tarjeta</i>), Otros (<i>controlar comunicación de campo cercano, tener acceso completo a la red, etc.</i>).
Citi Private Bank In View.	Android 1.7.1	Contactos(<i>consultar tus contactos</i>), Ubicación(<i>acceder a tu ubicación aproximada</i>), Teléfono (<i>consultar la identidad y el estado del teléfono</i>), Micrófono (<i>grabar sonido</i>), Otros (<i>Recopilar información de diagnóstico, tener acceso completo a la red, etc.</i>).
Amazonas Móvil by Banco Amazonas S.A.	Android 1.4.1	Cámara(<i>realizar fotografías y videos</i>), Contactos(<i>consultar tus contactos</i>), Ubicación(<i>acceder a tu ubicación aproximada</i>), Teléfono (<i>consultar la identidad y el estado del teléfono</i>), Almacenamiento (<i>modificar o eliminar contenido de la tarjeta</i>), Otros (<i>controlar comunicación</i>

		<i>de campo cercano, tener acceso completo a la red, etc.).</i>
Banca MOVIL (Banco Guayaquil).	Android 4.4	Cámara(<i>realizar fotografías y videos</i>), Ubicación(<i>acceder a tu ubicación aproximada</i>), Almacenamiento (<i>modificar o eliminar contenido de la tarjeta</i>), Otros (<i>impedir que el teléfono entre en modo suspenso, tener acceso completo a la red, etc.</i>)
Banco de Loja S. A	Android 1.0.2	Otros (<i>impedir que el teléfono entre en modo suspenso, tener acceso completo a la red, recibir datos de Internet, etc.</i>).
Banco Produbanco S.A	Android 2.6.2	Cámara(<i>realizar fotografías y videos</i>), Contactos(<i>consultar tus contactos</i>), Ubicación(<i>acceder a tu ubicación aproximada</i>), Teléfono (<i>consultar la identidad y el estado del teléfono</i>), Almacenamiento (<i>modificar o eliminar contenido de la tarjeta</i>).
Banco del Pacifico S.A	Android 4.1	Cámara(<i>realizar fotografías y videos</i>), Contactos(<i>consultar tus contactos</i>), Ubicación(<i>acceder a tu ubicación aproximada</i>), Teléfono (<i>consultar la identidad y el estado del teléfono</i>), Almacenamiento (<i>modificar o eliminar contenido de la tarjeta</i>), Otros (<i>controlar comunicación de campo cercano, tener acceso completo a la red, etc.</i>).
Banco Internacional S.A	Android 1.42	Ubicación (<i>acceder a tu ubicación aproximada</i>),

		Almacenamiento (<i>modificar o eliminar contenido de la tarjeta</i>), Otros (<i>controlar comunicación de campo cercano, tener acceso completo a la red, etc.</i>).
Banco del Pichincha S.A	Android 5.3	Cámara(<i>realizar fotografías y videos</i>), Micrófono (<i>grabar sonido</i>), Ubicación(<i>acceder a tu ubicación aproximada</i>), Teléfono (<i>consultar la identidad y el estado del teléfono</i>), Almacenamiento (<i>modificar o eliminar contenido de la tarjeta</i>), Otros (<i>controlar comunicación de campo cercano, tener acceso completo a la red, etc.</i>).

Nota: Permisos que pide el sistema Android a las Apps (elaboración propia)

4.1 Análisis de Seguridad en el Transporte de Envío de Datos

Un punto importante en la elaboración de aplicaciones móviles transaccionales es el uso de tipo de conexiones entre la aplicación y el servidor, la misma tiene que ser segura.

SSL/TLS es una tecnología simple y fácil de interpretarla al momento de desarrollar, pero no da garantía de la seguridad de información que viaja, para aquello se debe tener en cuenta dos aspectos claves.

- El certificado SSL/TLS debe ser manipulado de forma adecuada; debe ser firmado en base a un algoritmo seguro o fuerte (ASHA2), la cadena de conexión debe estar parametrizada de forma correcta para garantizar el no permitir un bypass en la autenticación correspondiente.

- Configuración bien definida; no contar con cifradores obsoletos o inseguros (es recomendable usar versiones actualizadas en base al protocolo SSL), el servidor debe estar configurado con algún cifrado (EDCHED, AES-GCM).

Es clave hacer uso de un proxy para medir el grado de seguridad y de comunicación que hay con el servidor final, en la figura 3 se muestra el uso de un proxy para verificar conexión.

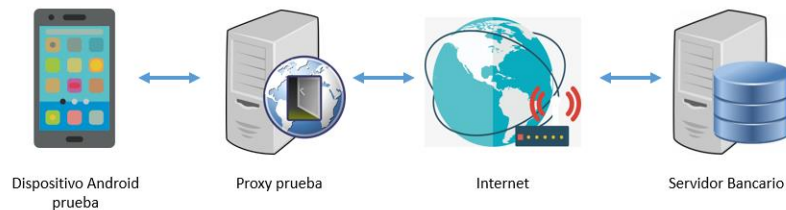


Figura 3 Uso proxy prueba para verificar conexión entre el cliente y el servidor

Fuente: Elaboración propia

Se hace uso de herramientas incluidas dentro del Sistema Operativo (Android SDK). Luego se procede a instalar un emulador de proxy *Wireshark* en la PC, este permite analizar el tráfico TCP/UDP y HTTP que se genera.

4.2 Análisis del comportamiento de las aplicaciones

Este punto es clave, se monta un ambiente el cual da acceso al análisis de puntos claves en el funcionamiento de la aplicación:

- Información que se almacena en la aplicación fuera de su área de almacenamiento (local o memoria SD).
- Información generada por el log.
- Información de certificados de entrada y salida.
- Información almacenada en el espacio de almacenamiento de la aplicación.

En la figura 4 podemos visualizar el escenario de estudio.

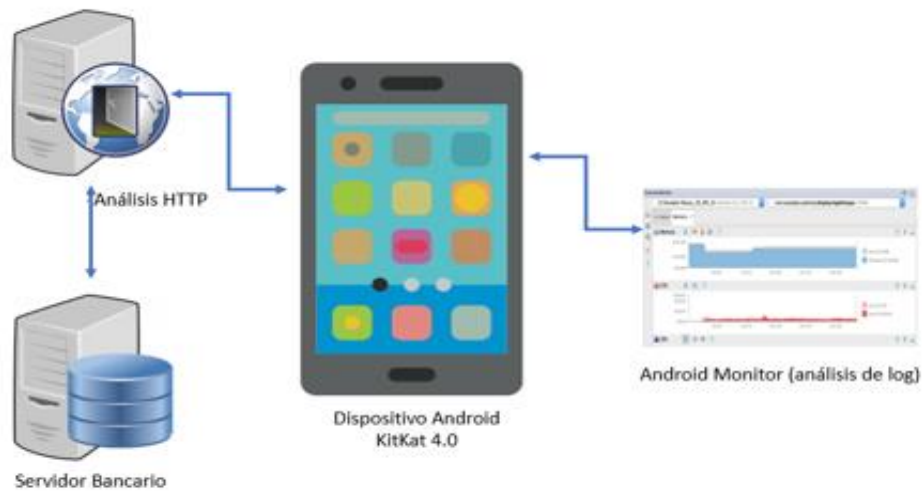


Figura 4 Configuración para el análisis.

Fuente: Elaboración propia

Para la elaboración de este análisis se requiere la colaboración de un cliente bancario cuya cuenta este activa. Una vez obtenida la parte del cliente se instala el emulador y el cliente realiza acciones básicas en el aplicativo.

- Logearse (login) en el aplicativo
- Revisión de cuenta ahorro o corriente.
- Revisión de su estado de cuenta de tarjetas.
- Realizar transferencias entre bancos distintos
- Mantener sin acción alguna la sesión iniciada en el aplicativo.

Como dato importante **Wireshark** es un analizador de protocolos que se encuentra disponible para plataformas Windows y Unix. Este analizador nos permite escuchar el tráfico que se genera en toda una red, a su vez analizar paquetes y realizar filtros de búsqueda.

4.2.1 Vulnerabilidades a encontrar

- Pérdida de paquetes tanto de recepción como de envío.
- Varias de estas aplicaciones procesan información y hacen el envío a través de un medio inseguro (HTTP y no HTTP'S), debido a que varias de estas aplicaciones hacen envío de información por medio de un texto plano HTTP, tenemos como ejemplo el envío de ubicación en tiempo real del usuario.

4.3 Análisis de tráfico procedente del aplicativo móvil del Banco del Pacifico.

Como primer paso seleccionamos la interfaz al cual vamos a visualizar todo el tráfico que se genera en la misma: en este caso la interfaz a filtrar es la wifi.

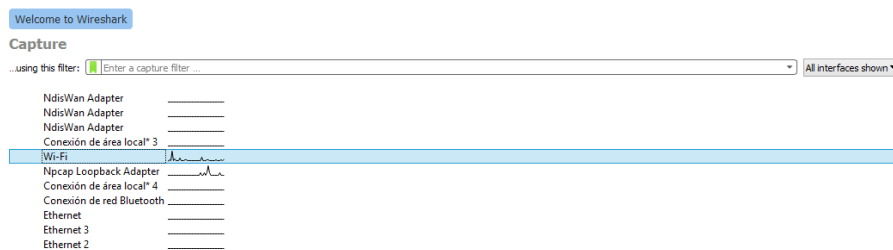
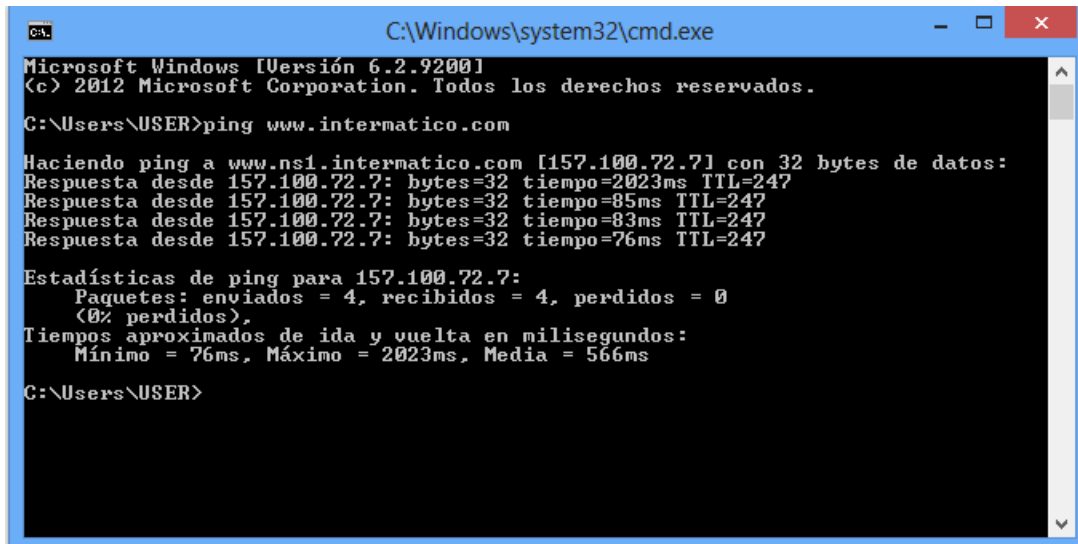


Figura 5 Seleccionamos interfaz a filtrar (WIFI)

Fuente: Elaboración propia

Como segundo paso necesitamos conocer cuál es la dirección IP pública de la banca virtual a ser analizada, en este caso (Banca Virtual-Banco del Pacifico).

Este paso lo realizamos haciendo uso del *Símbolo del sistema de Windows*, posterior a esto generamos un ping hacia el dominio principal de la banca móvil (ejemplo: www.intermatico.com), como respuesta tendremos la IP publica a buscar.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.2.9200]
(c) 2012 Microsoft Corporation. Todos los derechos reservados.

C:\Users\USER>ping www.intermatico.com

Haciendo ping a www.nsl.intermatico.com [157.100.72.7] con 32 bytes de datos:
Respuesta desde 157.100.72.7: bytes=32 tiempo=2023ms TTL=247
Respuesta desde 157.100.72.7: bytes=32 tiempo=85ms TTL=247
Respuesta desde 157.100.72.7: bytes=32 tiempo=83ms TTL=247
Respuesta desde 157.100.72.7: bytes=32 tiempo=76ms TTL=247

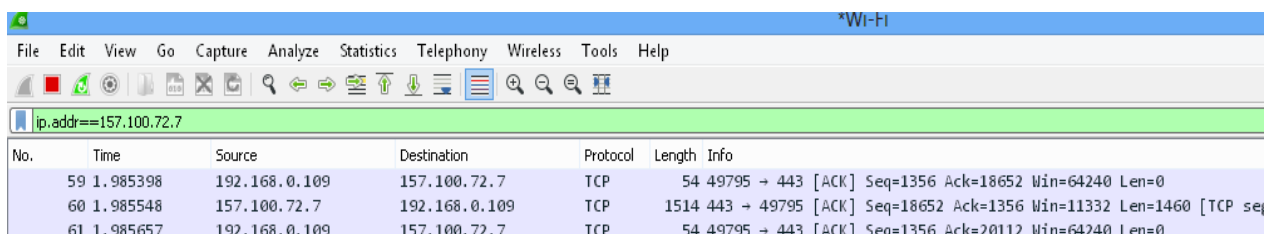
Estadísticas de ping para 157.100.72.7:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 76ms, Máximo = 2023ms, Media = 566ms

C:\Users\USER>
```

Figura 6 Ping hacia el dominio Banca Móvil Pacifico

Fuente: Elaboración propia

Una vez obtenida la dirección IP Publica procedemos a realizar un filtro dentro del aplicativo Wireshark, añadiéndole como parámetro de filtro la siguiente línea: *ip.addr==157.100.72.7*.



No.	Time	Source	Destination	Protocol	Length	Info
59	1.985398	192.168.0.109	157.100.72.7	TCP	54	49795 → 443 [ACK] Seq=1356 Ack=18652 Win=64240 Len=0
60	1.985548	157.100.72.7	192.168.0.109	TCP	1514	443 → 49795 [ACK] Seq=18652 Ack=1356 Win=11332 Len=1460 [TCP seq
61	1.985657	192.168.0.109	157.100.72.7	TCP	54	49795 → 443 [ACK] Seq=1356 Ack=20112 Win=64240 Len=0

Figura 7 Se añade filtro de dirección IP

Fuente: Elaboración propia

Con esto podremos escuchar todo el tráfico relacionado con la aplicación bancaria Banco del Pacifico, obteniendo como resultado los siguientes puntos.

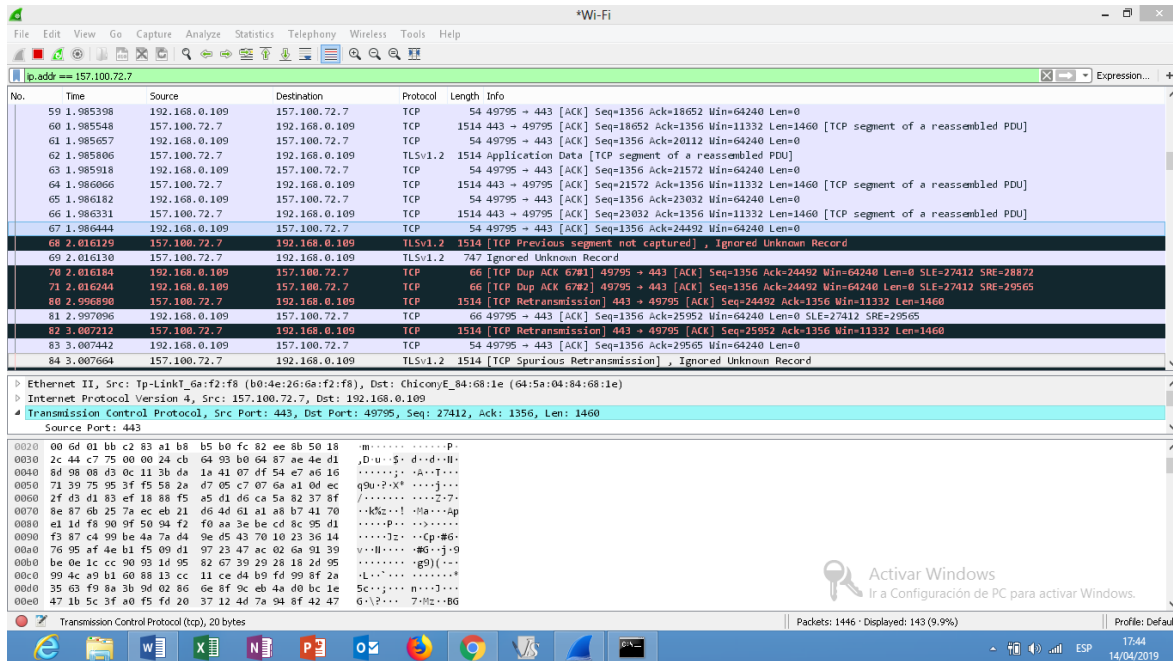


Figura 8 Resultados obtenidos con el filtro añadido

Fuente: Elaboración propia

Una vez obtenidos los resultados podemos interpretar los distintos resultados que nos genera esta aplicación, clasificándolos por color y por información.

Sabiendo que los de color celeste no tienen problema alguno, pero los de color rojo con negro si sufren variaciones, una ventaja de la aplicación Wireshark es que te informa al analizador sobre posibles falencias en los paquetes que se trafican añadiéndoles información de respuesta, por ejemplo:

66	1.986331	157.100.72.7	192.168.0.109	TCP	1514	443 → 49795 [ACK] Seq=23032 Ack=1356 Win=11332 Len=1460 [TCP segment of a reassembled PDU]
67	1.986444	192.168.0.109	157.100.72.7	TCP	54	49795 → 443 [ACK] Seq=1356 Ack=24492 Win=64240 Len=0
68	2.016129	157.100.72.7	192.168.0.109	TLSv1.2	1514	[TCP Previous segment not captured] , Ignored Unknown Record
69	2.016130	157.100.72.7	192.168.0.109	TLSv1.2	747	Ignored Unknown Record

Figura 9 Error de respuesta: Segmento no capturado

Fuente: Elaboración propia

Podemos deducir del siguiente resultado que hubo comunicación en tiempo real entre el cliente, en este caso Ip origen: 192.168.0.109 y el servidor Ip destino: 157.100.71.7, el envío se generó de manera efectiva, pero la respuesta por parte del servidor no fue exitosa ya que no se capturo segmento en el protocolo TLS en su versión 1.2.

81	2.997096	192.168.0.109	157.100.72.7	TCP	66 49795 → 443 [ACK] Seq=1356 Ack=25952 Win=64240 Len=0 SLE=27412 SRE=29565
82	3.007212	157.100.72.7	192.168.0.109	TCP	1514 [TCP Retransmission] 443 → 49795 [ACK] Seq=25952 Ack=1356 Win=11332 Len=1460

Figura 10 Error de retransmisión Aplicativo Móvil Pacifico

Fuente: Elaboración propia

Como segundo error podemos visualizar en la gráfica que existe un error de retransmisión, el mismo se basa en no poder tener una respuesta inmediata a una petición, lo que conlleva a que el usuario insista en tener una respuesta (recargar menús) dentro del aplicativo bancario.

4.4 Análisis de tráfico procedente del aplicativo móvil del Banco de Guayaquil.

Como primer paso seleccionamos la interfaz al cual vamos a visualizar todo el tráfico que se genera en la misma: en este caso la interfaz a filtrar es la wifi.

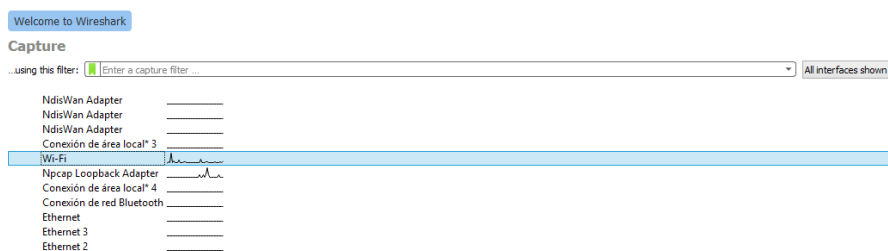
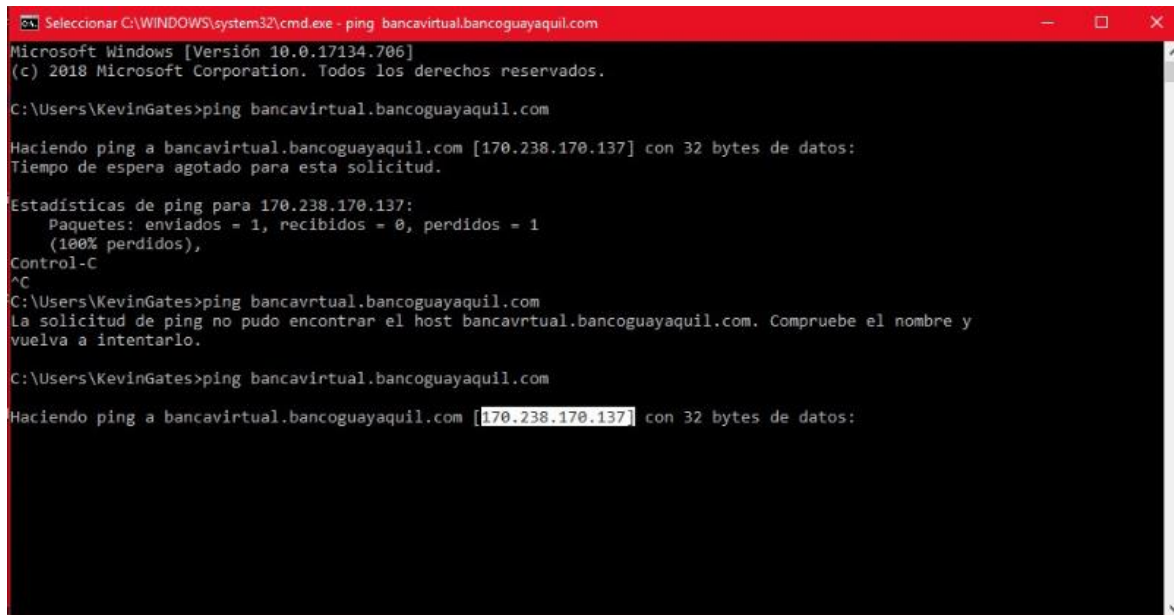


Figura 11 Seleccionamos interfaz a filtrar (WIFI)

Fuente: Elaboración propia

Como segundo paso necesitamos conocer cuál es la dirección IP pública de la banca virtual a ser analizada, en este caso (Banca Virtual-Banco del Guayaquil).

Este paso lo realizamos haciendo uso del *Símbolo del sistema de Windows*, posterior a esto generamos un ping hacia el dominio principal de la banca móvil (ejemplo: bancavirtual.bancoguayaquil.com), como respuesta tendremos la IP publica a buscar.



```
Selecccionar C:\WINDOWS\system32\cmd.exe - ping bancavirtual.bancoguayaquil.com
Microsoft Windows [Versión 10.0.17134.706]
(c) 2018 Microsoft Corporation. Todos los derechos reservados.

C:\Users\KevinGates>ping bancavirtual.bancoguayaquil.com

Haciendo ping a bancavirtual.bancoguayaquil.com [170.238.170.137] con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 170.238.170.137:
    Paquetes: enviados = 1, recibidos = 0, perdidos = 1
              (100% perdidos),
Control-C
^C
C:\Users\KevinGates>ping bancavrtual.bancoguayaquil.com
La solicitud de ping no pudo encontrar el host bancavrtual.bancoguayaquil.com. Compruebe el nombre y
vuelva a intentarlo.

C:\Users\KevinGates>ping bancavirtual.bancoguayaquil.com

Haciendo ping a bancavirtual.bancoguayaquil.com [170.238.170.137] con 32 bytes de datos:
```

Figura 12 Ping hacia el dominio Banca Móvil Guayaquil

Fuente: Elaboración propia

Una vez obtenida la dirección IP Publica procedemos a realizar un filtro dentro del aplicativo Wireshark, añadiéndole como parámetro de filtro la siguiente línea: *ip.addr==170.238.17.137*.



Figura 13 Filtro con dirección IP publica de la banca móvil

Fuente: Elaboración propia

Con esto podremos escuchar todo el tráfico relacionado con la aplicación bancaria Banco de Guayaquil, obteniendo como resultado los siguientes puntos.

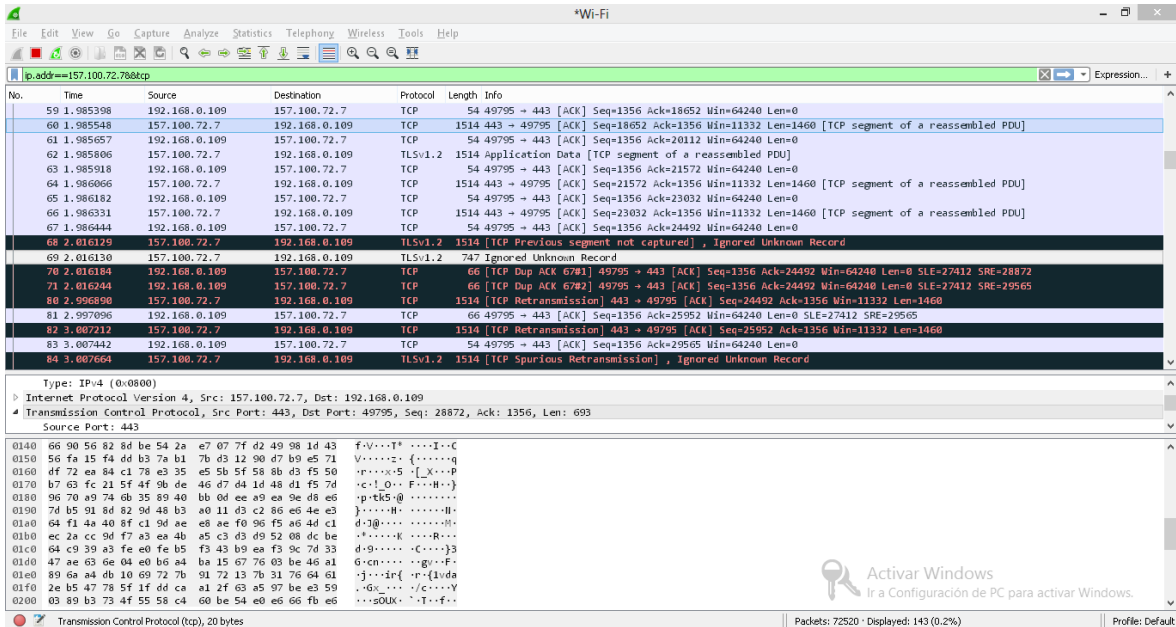


Figura 14 Tráfico generado por parte de la banca Móvil

Fuente: Elaboración propia

Una vez obtenido los resultados podemos interpretar los distintos resultados que nos genera esta aplicación, clasificándolos por color y por información.

Sabiendo que los de color celeste no tienen problema alguno, pero los de color rojo con negro si sufren variaciones, una ventaja de la aplicación Wireshark es que te informa al analizador sobre posibles falencias en los paquetes que se trafican añadiéndoles información de respuesta, por ejemplo:

No.	Time	Source	Destination	Protocol	Length	Info
366	103.592182	170.238.170.137	192.168.0.101	TCP	54	443 → 2035 [FIN, PSH, ACK] Seq=1 Ack=2 Win=32764 Len=0
367	103.593263	192.168.0.101	170.238.170.137	TCP	54	2035 → 443 [ACK] Seq=2 Ack=2 Win=68 Len=0
372	108.611889	170.238.170.137	192.168.0.101	TCP	54	443 → 2036 [FIN, PSH, ACK] Seq=1 Ack=2 Win=32848 Len=0
374	108.612335	192.168.0.101	170.238.170.137	TCP	54	2036 → 443 [ACK] Seq=2 Ack=2 Win=68 Len=0
450	148.593634	192.168.0.101	170.238.170.137	TCP	55	[TCP Keep-Alive] 2035 → 443 [ACK] Seq=1 Ack=2 Win=68 Len=1
451	148.647795	170.238.170.137	192.168.0.101	TCP	54	[TCP Keep-Alive ACK] 443 → 2035 [ACK] Seq=2 Ack=2 Win=32764 Len=0
487	153.612143	192.168.0.101	170.238.170.137	TCP	55	[TCP Keep-Alive] 2036 → 443 [ACK] Seq=1 Ack=2 Win=68 Len=1
488	153.619923	170.238.170.137	192.168.0.101	TCP	54	[TCP Keep-Alive ACK] 443 → 2036 [ACK] Seq=2 Ack=2 Win=32848 Len=0
630	193.432192	192.168.0.101	170.238.170.137	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (no response found!)

Figura 15. Análisis de resultados por protocolo ICMP

Fuente: Elaboración propia

Como dato curioso al realizar el análisis de paquetes en la aplicación banca móvil Guayaquil podemos notar que existe un bloqueo del protocolo ICMP, el cual no permite realizar el test ping para verificar la comunicación entre el cliente y el servidor. Esto genera que Wireshark detecte un error de ICMP, añadiendo como mensaje de información que no existe una respuesta ICMP.

4.5 Análisis estático del aplicativo (APK)

Mediante el estudio estático del APK generado por la App y teniendo a la mano las clases y métodos es posible realizar dos tipos de análisis en la aplicación:

Como primer análisis se tiene el estudio estático modificado a cerca de las clases de JAVA haciendo uso de herramientas de análisis como *Findbugs*, esta va de la mano con un plugin asociado llamado Bugs Find Security, el mismo permite y se especializa en encontrar vulnerabilidades de seguridad y poder aplicar una mejora en esa parte del código de FindBugs.

Básicamente el segundo análisis es más directo al tratarse de un estudio analítico estático y manual de la aplicación basada en JAVA con el fin de buscar información clave como la que mencionamos a continuación:

- Carga de información a archivos logs.
- Uso de certificados obsoletos o en reposo.
- URL'S visibles a conexiones con servidores.

4.5.1 Vulnerabilidades a encontrar

- Mal uso de nomenclatura a las clases o métodos: genera confusión o incluso errores al momento de compilar la aplicación y llevarla a prueba.
- Paquetes muertos o perdidos al realizar conexión con los servidores o realizar peticiones de manera local con el dispositivo móvil.
- URL mal especificadas o visibles a conexión con el servidor: genera una posible inyección por parte de personal externo con malas intenciones y perjuicios para los clientes.
- Errores de código procedentes del uso de métodos o mal llamado de clases, creaciones de instancias y uso de una mala programación.
- Carga de información a archivos de texto con información actualizada de procesos que genera la aplicación.

Como primer paso para este análisis tenemos que descargar todas las APK de las aplicaciones bancarias correspondientes.

- AF3DWBexsd0viV96e5U9-SkM_V5zB6ozmFWUQHc2ivcljm9S1I_JjmlM9...
- citi-mobile - FilePlanet.apk
- com.bancodeguayaquil.apk
- com.bayteq.be.produbanco-v2.1.1.apk
- com.bayteq.loja.bancamovil_12.apk
- com.pacifico.iwant_2019-03-21.apk
- dinama.practiEfectivo.android.internacional_2017-05-16 (1).apk
- movilmatico.pacifico-4.1.apk

Figura 16. Descargas de los APK de los aplicativos

Fuente: Elaboración propia

Como segundo paso para este análisis es indispensable hacer uso de un IDE para visualización del APK y análisis del mismo por el cual se ha procedido a utilizar eclipse, a su vez se instala un plugin llamado FindBugs.

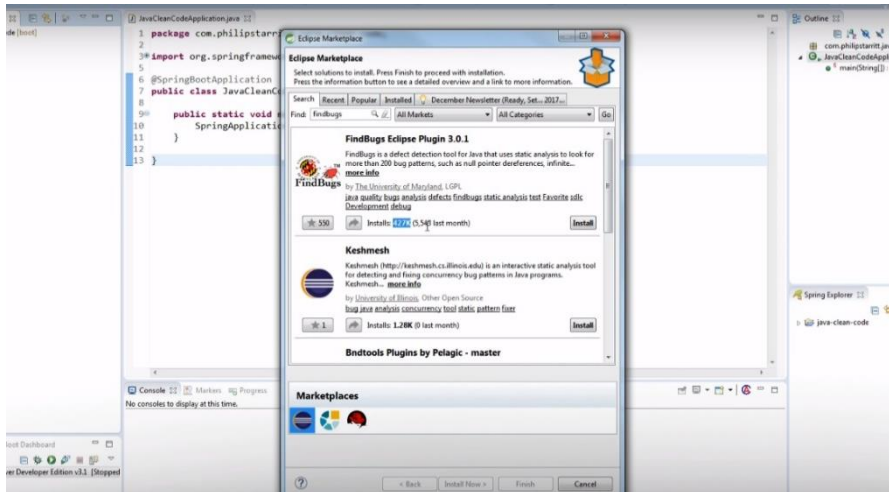


Figura 17. Eclipse y su plugin FindBugs

Fuente: Elaboración propia

Una vez teniendo instalado el plugin se reinicia el IDE y se procede a abrir el archivo de la aplicación, como se podrá visualizar en la siguiente imagen en el archivo context.html se muestra información de la aplicación.

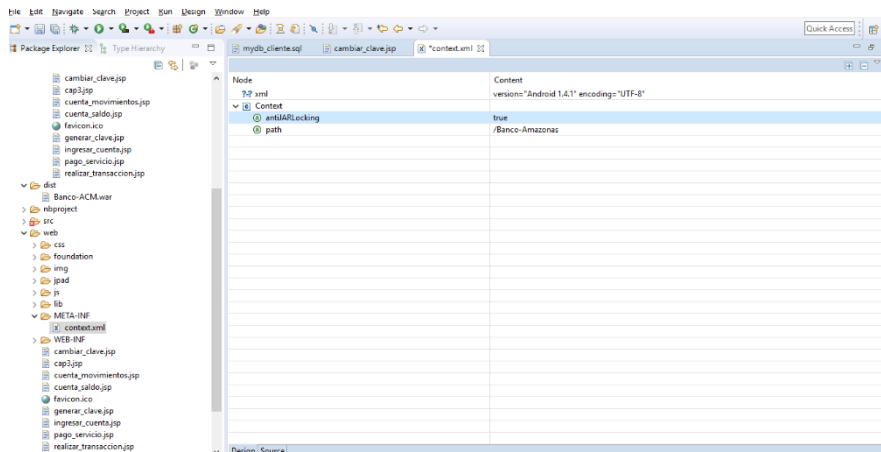


Figura 18. Archivo con información base del aplicativo

Fuente: Elaboración propia

Para el correcto funcionamiento del plugin es indispensable activar ciertos parámetros, los cuales están definidos en la configuración de cada proyecto

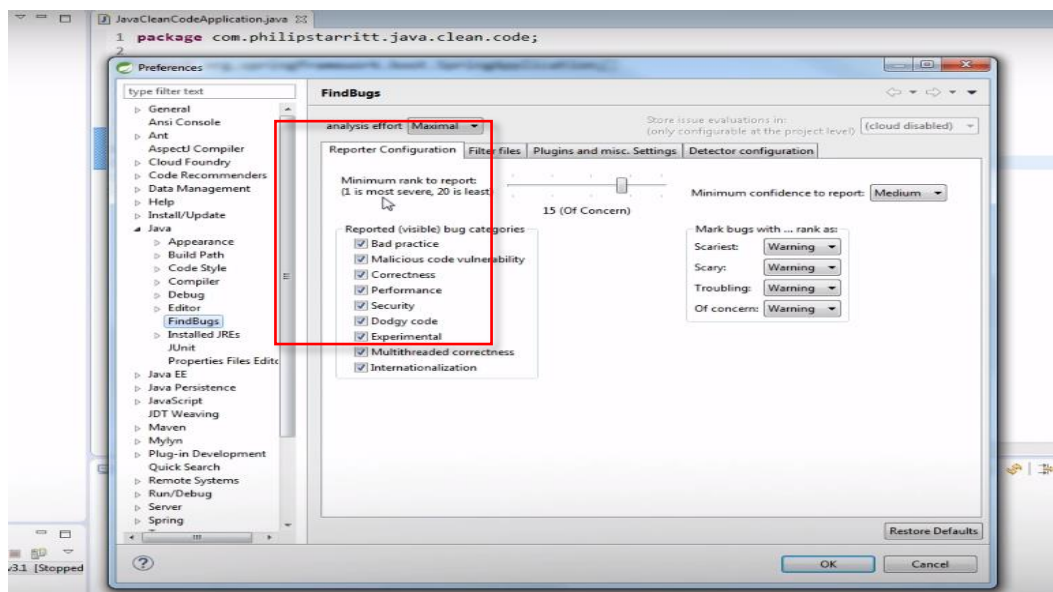


Figura 19 Configuración en el proyecto del aplicativo

Fuente: Elaboración propia

En este apartado fijarse bien que el casillero este correctamente seleccionado.

Creamos un proyecto nuevo donde será nombrado por cada banco para su respectivo análisis.

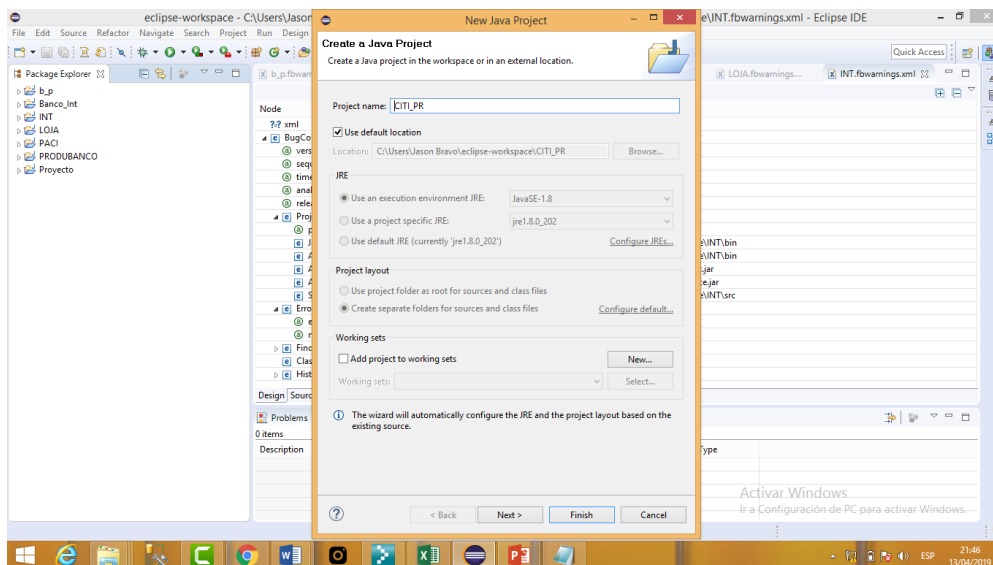


Figura 20 Proyecto base

Fuente: Elaboración propia

Abriremos la carpeta ‘eclipse-workspace’ donde estarán los proyectos recién creados y dentro de la carpeta creada ‘CITI_PR’, ubicare el APK correspondiente del banco asignado, Al actualizar en eclipse el APK estará ya asignado en el IDE.

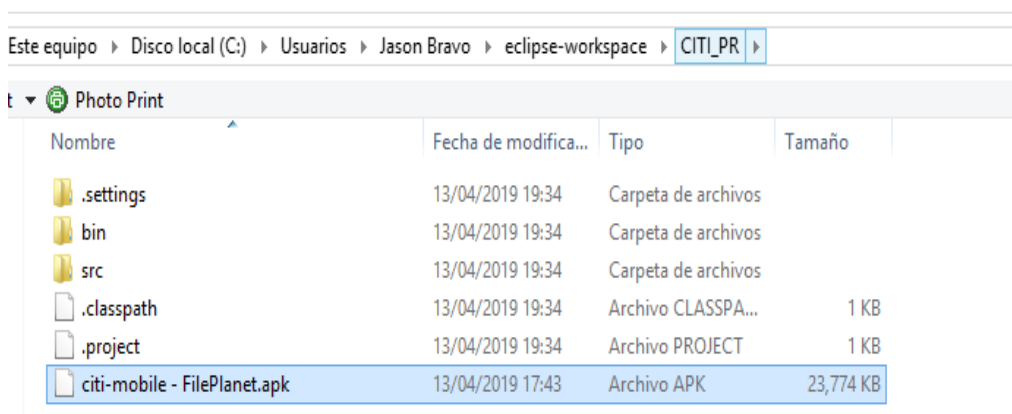


Figura 21. APK a la raíz del proyecto

Fuente: Elaboración propia

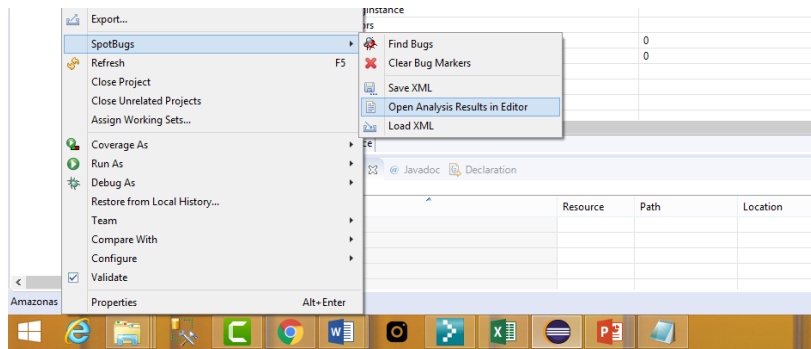


Figura 23. Resultados de Fing Bugs

Fuente: Elaboración propia

Esta imagen nos genera los bugs con los que cuenta la aplicación de manera global, específicamente los bugs generados por instancias como podemos tener:

Paquetes muertos o perdidos de forma local, errores al nombrar clases (comúnmente al usar una mala nomenclatura de clase); otro error notorio es el uso de una versión obsoleta del sistema operativo, errores de URL pérdidas o no bien definidas.

Los resultados que nos genera este plugin, no contiene ningún error por lo cual se puede realizar un mejor análisis.

En la aplicación móvil bancaria Banco Pichincha, la cual está basada en Android en su versión 5.3, a su vez haciendo uso de las herramientas, pasos mencionados anteriormente y clasificar su nivel de seguridad.

lode	Content
?-? xml	version="1.0" encoding="UTF-8"
[-] BugCollection	
[+] version	4.0.0-beta1
[+] sequence	1
[+] timestamp	1555177241905
[+] analysisTimestamp	1555177241437
[+] release	
[-] Project	
[-] Errors	
[+] errors	0
[+] missingClasses	0
[-] FindBugsSummary	
[-] ClassFeatures	
[-] History	

Figura 24 Resultados App Banco Pichincha

Fuente: Elaboración propia

Los resultados que nos genera este plugin, no contienen ningún error por lo cual se puede realizar un mejor análisis.

En la aplicación móvil bancaria Produbanco, la cual está basada en Android en su versión 1.4.2, a su vez haciendo uso de las herramientas y pasos mencionados anteriormente y clasificar su nivel de seguridad.

[-] BugInstance	
[-] BugInstance	
[-] BugInstance	
[-] Errors	
[+] errors	0
[+] missingClasses	0
[-] FindBugsSummary	
[-] ClassFeatures	
[-] History	

Figura 25 Resultados App Banco Produbanco

Fuente: Elaboración propia

Los resultados no generaron errores por lo cual se verificó sus respectivas características y un buen análisis.

En la aplicación móvil Citi Private Bank In View, la cual está basada en Android en su versión 1.7.1, a su vez haciendo uso de las herramientas y pasos mencionados anteriormente y clasificar su nivel de seguridad.

Node	Content
??.xml	version="1.0" encoding="UTF-8"
BugCollection	
version	4.0.0-beta1
sequence	1
timestamp	1555356297506
analysisTimestamp	1555356289202
release	
Project	
Errors	
errors	0
missingClasses	0
FindBugsSummary	
ClassFeatures	
History	

Figura 267 Resultados de la App Citi Bank

Fuente: Elaboración propia

Node	Content
AuxClasspathEntry	C:\Program Files\Java\jre1.8.0_202\lib\rt.jar
AuxClasspathEntry	C:\Program Files\Java\jre1.8.0_202\lib\jce.jar
SrcDir	C:\Users\Jason Bravo\workspace\CITI_PR\src
Errors	
errors	0
missingClasses	0
FindBugsSummary	
timestamp	Sat, 13 Apr 2019 19:35:04 +0200
total_classes	0
referenced_classes	0
total_bugs	0
total_size	0
num_packages	0
java_version	1.8.0_202
vm_version	25.202-b08
cpu_seconds	4.61
clock_seconds	2.29
peak_mbytes	502.62
alloc_mbytes	1024.00
nr_seconds	0.00

Figura 27 Parámetros obtenidos

Fuente: Elaboración propia

En este análisis no hubo ningún error por lo cual se verificó sus respectivas características y un buen análisis.

En la aplicación móvil bancaria Banco Internacional, la cual está basada en Android en su versión 1.4.2, a su vez haciendo uso de las herramientas y pasos mencionados anteriormente y clasificar su nivel de seguridad.

Node	Content
Project	
Errors	
errors	0
missingClasses	0
FindBugsSummary	
timestamp	Sat, 13 Apr 2019 22:21:58 +0200
total_classes	0
referenced_classes	0
total_bugs	0
total_size	0
num_packages	0
java_version	1.8.0_202
vm_version	25.202-b08
cpu_seconds	0.52
clock_seconds	0.24
peak_mbytes	519.46
alloc_mbytes	1024.00
gc_seconds	0.00
FindBugsProfile	
ClassFeatures	

Figura 28 Resultado App Banco Internacional

Fuente: Elaboración propia

Los resultados que nos genera este plugin para la App del Banco Internacional, no contienen ningún error por lo cual se puede realizar un mejor análisis.

En la aplicación móvil bancaria Banco de Loja, la cual está basada en Android en su versión 1.0.2, a su vez haciendo uso de las herramientas y pasos mencionados anteriormente y clasificar su nivel de seguridad.

Node	Content
Project	
Errors	
errors	0
missingClasses	0
FindBugsSummary	
timestamp	Sat, 13 Apr 2019 19:39:27 +0200
total_classes	0
referenced_classes	0
total_bugs	0
total_size	0
num_packages	0
java_version	1.8.0_202
vm_version	25.202-b08
cpu_seconds	1.14
clock_seconds	0.49
peak_mbytes	511.09
alloc_mbytes	1024.00
gc_seconds	0.00
FindBugsProfile	
ClassFeatures	

Figura 29 Resultados App Banco de Loja

Fuente: Elaboración propia

Los resultados que nos genera este plugin para la App del Banco de Loja, no contiene ningún error por lo cual se puede realizar un mejor análisis.

En la aplicación móvil bancaria Banco Bolivariano, la cual está basada en Android en su versión 4.4, a su vez haciendo uso de las herramientas y pasos mencionados anteriormente y clasificar su nivel de seguridad.

Node	Content
SrcDir	C:\Users\Jason Bravo\workspace\bol\src
Errors	
errors	0
missingClasses	0
FindBugsSummary	
timestamp	Sun, 14 Apr 2019 11:28:07 +0200
total_classes	0
referenced_classes	0
total_bugs	0
total_size	0
num_packages	0
java_version	1.8.0_202
vm_version	25.202-b08
cpu_seconds	0.69
clock_seconds	0.26
peak_mbytes	520.18
alloc_mbytes	1024.00
gc_seconds	0.03
FindBugsProfile	
ClassFeatures	

Figura 30 Resultado App Banco Bolivariano

Fuente: Elaboración propia

Los resultados que nos genera este plugin para la App del Banco Bolivariano, no contienen ningún error por lo cual se puede realizar un mejor análisis.

En la aplicación móvil bancaria Banco del Pacifico, la cual está basada en Android en su versión 4.1, a su vez haciendo uso de las herramientas y pasos mencionados anteriormente y clasificar su nivel de seguridad.

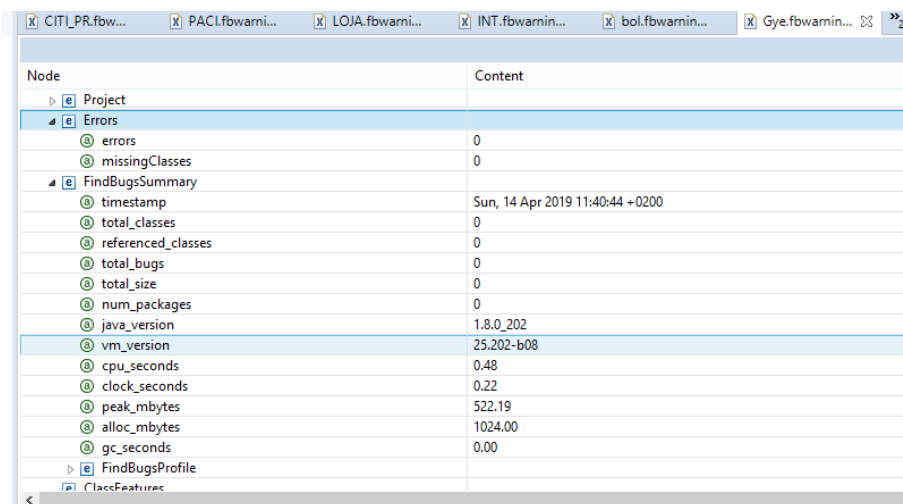
Node	Content
SrcDir	C:\Users\Jason Bravo\workspace\PACI\src
Errors	
errors	0
missingClasses	0
FindBugsSummary	
timestamp	Sat, 13 Apr 2019 19:37:47 +0200
total_classes	0
referenced_classes	0
total_bugs	0
total_size	0
num_packages	0
java_version	1.8.0_202
vm_version	25.202-b08
cpu_seconds	1.56
clock_seconds	0.56
peak_mbytes	507.75
alloc_mbytes	1024.00
gc_seconds	0.04
FindBugsProfile	
ClassFeatures	

Figura 31 Resultado Banco de Pacifico

Fuente: Elaboración propia

Los resultados que nos genera este plugin para la App del Banco del Pacifico, no contiene ningún error por lo cual se puede realizar un mejor análisis.

En la aplicación móvil bancaria Banco de Guayaquil, la cual está basada en Android en su versión 4.4, a su vez haciendo uso de las herramientas y pasos mencionados anteriormente y clasificar su nivel de seguridad.



Node	Content
Project	
Errors	
errors	0
missingClasses	0
FindBugsSummary	
timestamp	Sun, 14 Apr 2019 11:40:44 +0200
total_classes	0
referenced_classes	0
total_bugs	0
total_size	0
num_packages	0
java_version	1.8.0_202
vm_version	25.202-b08
cpu_seconds	0.48
clock_seconds	0.22
peak_mbytes	522.19
alloc_mbytes	1024.00
gc_seconds	0.00
FindBugsProfile	
ClassFeatures	

Figura 32 Resultados App Banco Guayaquil

Fuente: Elaboración propia

Los resultados que nos genera este plugin para la App del Banco Guayaquil, no contienen ningún error por lo cual se puede realizar un mejor análisis.

CAPÍTULO 5

CONCLUSIONES

En este análisis se observa que un 44% de las aplicaciones analizadas utilizan tecnologías biométricas y cada uno de los aplicativos utiliza una versión Android más actualizada. Después de los análisis encontrados en dichos aplicativos con el plugin *FindBugs*, no se detectó errores, lo que conlleva al usuario un cierto grado de seguridad y confiabilidad de estos aplicativos. Estas aplicaciones bancarias han provocado un giro a nivel nacional que en realidad es muy beneficioso para el consumidor. Cada aplicación da a conocer al usuario sobre políticas y permisos antes de ponerla en funcionamiento para los clientes.

El análisis realizado mediante el uso de *Wireshark* tenemos noción más amplia de cómo se genera el tráfico entre el servidor bancario y el cliente final. En los resultados alojados por el mismo, en el tráfico de datos se pudo encontrar ciertos errores (retransmisión, segmentos no capturados) que son comunes en estas aplicaciones, debido a la gran cantidad de tráfico en tiempo real entre el cliente-servidor lo que conlleva a que la banca digital detecten falencias durante la ejecución de una transacción o alguna petición en general.

Una de las ventajas de este aplicativo es que da a conocer al analizador sobre posibles falencias en los paquetes que circulan por la red, obteniendo resultados entendibles para los analizadores de las mismas, así cumplir nuestras expectativas de seguridad en un ambiente amigable.

REFERENCIAS BIBLIOGRÁFICAS

Bibliografía

- Andreu, J. (2007). *Gestión de servidores web (Servicios en red)*. Madrid: Editex.
- Apress. (2013). *Pro C++ with the NDK*. Santiago: Onur Cinar.
- Avilés, G. G. (2015). *Seguridad en Bases de Datos y Aplicaciones Web*. Bogota: IT Campus Academy.
- Cabello, A. L. (2015). *Desarrollo de aplicaciones web distribuidas. IFCD0210*. Lima: IC Editorial.
- Cambria, E. (2013). *Extreme Learning Machines*. La paz: IEEE Intelligent Systems.
- Consulting, i. (2015). *Desarrollo Profesional de Aplicaciones Web con ASP.NET*. Ambato: Consulting IKor.
- Díaz, N. Y. (2015). *Heurísticas para evaluar la usabilidad de aplicaciones web bancarias*. Lima: Pontificia Universidad Católica del Perú,.
- E, A. (2014). *Introduction to machine learning*. Madrid: MIT press.
- Escudero J, I. E. (2013). *Machine learning-based method for personalized and cost-effective detection of Alzheimer's disease*. New York: IEEE Transactions on Bio-Medical Engineering.
- Groussard, T. (2010). *Java Enterprise Edition: Desarrollo de aplicaciones web con JEE 6*. Madrid: Ediciones ENI.
- H. K. Ham, Y. B. (2011). *Mobile application compatibility test system design for android*. Springer: Continuity Education.
- Hevia, A. (2009). *CC51D - Seguridad de Datos*. Santiago de Chile: Editorial de Chile.
- J. H. Saltzer, M. D. (2000). *The protection of information in computer systems*. New York: Preceeding of IEEE.

- Jaime Rivera Camino, M. d.-R. (2014). *Marketing sectorial. Principios y aplicaciones*. New York: ESIC Editorial.
- R. Johnson, Z. W. (2012). *Analysis of android applications*. Manhattan: IEEE Sixth.
- Robles, J. T. (2015). *Los bancos de imágenes en internet: características, funciones y aplicaciones*. Madrid: Bibtex.
- Scotka, R. (10 de 02 de 2014). *Shining a flashlight on mobile application permissions*. Obtenido de <https://www.veracode.com/blog/2014/04/shining-a-flashlight-on-mobile-application-permissions>
- Villoria, L. N. (2009). *APLICACIONES WEB 2.0 - Google docs*. New York: Google Docs.
- Vishwanahan, A. S. (2017). *Introduccion a Learning Machine*. Madrid: Smola.
- Y. Shao, X. L. (2014). *Rootguard: Protecting rooted android phones*. Bogota: Computer IEEE.

Urkund Analysis Result

Analysed Document: urkund.docx (D50683978)
Submitted: 4/15/2019 3:29:00 AM
Submitted By: gandradet@unemi.edu.ec
Significance: 0 %

Sources included in the report:

Instances where selected sources appear:

0



REGISTRO DE ACOMPAÑAMIENTOS

Inicio: 05-11-2018 Fin 30-04-2019

FACULTAD CIENCIAS DE LA INGENIERIA

CARRERA: INGENIERÍA EN SISTEMAS COMPUTACIONALES

Línea de investigación: DESARROLLO DE SOFTWARE, SEGURIDAD DE LA INFORMACIÓN.

TEMA: ANÁLISIS DE ENTORNO A LA SEGURIDAD DE LOS DISPOSITIVOS BIOMÉTRICOS EN APLICACIONES BANCARIAS

ACOMPAÑANTE: BRAVO DUARTE FREDDY LENIN

DATOS DEL ESTUDIANTE			
Nº	APELLIDOS Y NOMBRES	CÉDULA	CARRERA
1	ANDRADE TOSCANO GERARDO DAVID	0942192907	INGENIERÍA EN SISTEMAS COMPUTACIONALES
2	BRAVO PIÑA JASON ANTONIO	0919131011	INGENIERÍA EN SISTEMAS COMPUTACIONALES

Nº	FECHA	HORA		Nº HORAS	DETALLE
1	2019-09-01	Inicio: 15:59 p.m.	Fin: 17:59 p.m.	2	REVISION DE TEMA Y CAPITULO 1
2	2019-12-02	Inicio: 15:27 p.m.	Fin: 17:27 p.m.	2	REVISION DE AVANCES DE APPLICATIVOS DE INGENIERIA INVERSA EN EL ANALISIS DE APP BANCARIAS


 BRAVO DUARTE FREDDY LENIN
 PROFESOR(A)


 REA SANCHEZ VICTOR HUGO
 DIRECTOR(A)


 ANDRADE TOSCANO GERARDO DAVID
 ESTUDIANTE


 BRAVO PIÑA JASON ANTONIO
 ESTUDIANTE

Dirección: Cdla. Universitaria Km. 1 1/2 vía km. 26
Conmutador: (04) 2715081 - 2715079 Ext. 3107
Telefax: (04) 2715187
 Milagro • Guayas • Ecuador

VISIÓN
 Ser una universidad de docencia e investigación.

MISIÓN
 La UNEMI forma profesionales competentes con actitud proactiva y valores éticos, desarrolla investigación relevante y oferta servicios que demanda el sector externo, contribuyendo al desarrollo de la sociedad.

