

Tabla de contenido

Resumen	i
Dedicatoria	v
1. Introducción	1
Motivación y aporte	2
2. Estado del Arte y Antecedentes	5
Seguridad de software	5
La triada CIA	5
Identificación, autenticación y autorización	6
El ciclo de vida del desarrollo de software (SDLC)	7
Principios de seguridad de sistemas	8
Desarrollo de aplicaciones móviles	10
Aplicaciones web móviles	11
Aplicaciones nativas	11
Aplicaciones híbridas	11
Aplicaciones web embebidas	12
Privacidad de información personal y del equipo móvil	12
La plataforma Android	13
Versiones	13
Arquitectura	15

Marco de aplicaciones	16
Aplicaciones	17
Almacenamiento	17
Seguridad y privacidad en Android	17
Permisos	17
Fragmentación	19
Instalación de aplicaciones maliciosas	20
Trabajo Relacionado	22
3. Definición del problema	25
Objetivo general	25
Objetivos específicos	25
4. Metodología	27
Selección de aplicaciones a analizar	27
Determinación de vulnerabilidades a buscar	28
Ingeniería reversa de la aplicación y análisis de transporte	30
Análisis estático del código fuente	31
Análisis de seguridad en el transporte de información	31
Análisis pasivo del comportamiento de la aplicación	33
Confeción de informes y de tesis	35
Vulnerabilidades y malas prácticas	35
Generación de tesis e informe de vulnerabilidades a bancos	36
Entrega de informe de vulnerabilidades a bancos	37
5. Resultados del análisis de aplicaciones móviles bancarias	39
6. Vulnerabilidades encontradas	43
Vulnerabilidades asociadas a abuso de permisos	43
V1: Acceso a contactos del usuario	43

V2: Acceso a información acerca de otras aplicaciones en uso	44
V3: Acceso al estado del teléfono	44
V4: Escritura en el almacenamiento externo del teléfono	44
V5: Lectura de logs del sistema	45
V6: Uso de georreferenciación	45
Vulnerabilidades asociadas a mal uso de conexiones HTTPS con el servidor .	46
V7: Cadena de certificación HTTPS mal hecha	46
V8: Carencia de Forward Secrecy	47
V9: CRIME	47
V10: Uso del cifrador RC4	47
V11: POODLE y uso del protocolo SSL3	48
V12: Falta de protección ante downgrades de protocolo	48
V13: No uso del protocolo TLS1.2	48
Otras vulnerabilidades	49
V14: Abuso de logging (código de pruebas olvidado)	49
V15: Actualización insegura de información (mediante HTTP)	50
V16: Almacenamiento de información sensible en base de datos SQLite o preferencias	50
V17: Almacenamiento de información sensible en cache	51
V18: Envío de información sensible a través de canal inseguro (HTTP) .	51
V19: Exceso de confianza en medidas anti-ingeniería reversa	51
V20: Falta de timeout	51
V21: Timeout mal implementado	52
V22: Mal uso de cifrado en reposo	53
V23: Mal uso de cifrado redundante	54
V24: Potencial Tampering de datos	54
V25: Uso innecesario del PAN de Tarjeta de Crédito en tránsito	56

7. Taxonomía de malas prácticas	57
Abuso en el uso de información personal de los usuarios	57
Buenas prácticas asociadas	58
Mal uso de cifrado	58
Buenas prácticas asociadas	59
Falta de protección de información sensible almacenada en el teléfono	59
Buenas prácticas asociadas	60
Falsa sensación de seguridad en el uso de SSL/TLS	60
Buenas prácticas asociadas	61
Código abandonado	63
Buenas prácticas asociadas	64
Uso de medidas anti-ingeniería reversa como medida de seguridad	64
Buenas prácticas asociadas	64
Abuso de privilegios	65
Buenas prácticas asociadas	65
8. Recomendaciones de seguridad para el desarrollo de aplicaciones móviles	67
Considerar el ambiente de operación de la aplicación	67
Tener cuidado respecto del almacenamiento de información en el aparato	68
Remover código de debugging o logging	69
Preocuparse de la calidad de la conexión	69
Implementar Timeouts	70
Analizar la seguridad de las dependencias (bibliotecas, frameworks)	71
Analizar la seguridad en el código propio	71
Tener en cuenta la privacidad en el uso de georreferenciación	72
Evitar el abuso de privilegios	72
Principio de Diseño Abierto	72
9. Futuras líneas de investigación	73

10. Conclusiones	75
Bibliografía	77
Anexo: Informes entregados a los bancos	83
Informe Banco 1	83
Introducción	83
Detalles de la aplicación analizada	84
Vulnerabilidades encontradas y su mitigación	84
Recursos interesantes	90
Informe Banco 2	91
Introducción	91
Detalles de la aplicación analizada	91
Vulnerabilidades encontradas y su mitigación	91
Recursos interesantes	97
Informe Banco 3	98
Introducción	98
Detalles de la aplicación analizada	98
Vulnerabilidades encontradas y su mitigación	99
Recursos interesantes	104
Informe Banco 4	105
Introducción	105
Detalles de la aplicación analizada	105
Vulnerabilidades encontradas y su mitigación	105
Recursos interesantes	110
Informe Banco 5	111
Introducción	111
Detalles de la aplicación analizada	111
Vulnerabilidades encontradas y su mitigación	111

Recursos interesantes	115
Informe Banco 6	116
Introducción	116
Detalles de la aplicación analizada	116
Vulnerabilidades encontradas y su mitigación	116
Recursos interesantes	122
Informe Banco 7	122
Introducción	122
Detalles de la aplicación analizada	123
Vulnerabilidades encontradas y su mitigación	123
Recursos interesantes	128
Informe Banco 8	129
Introducción	129
Detalles de la aplicación analizada	129
Vulnerabilidades encontradas y su mitigación	129
Recursos interesantes	135
Informe Banco 9	136
Introducción	136
Detalles de la aplicación analizada	136
Vulnerabilidades encontradas y su mitigación	136
Recursos interesantes	141
Informe Banco 10	142
Introducción	142
Detalles de la aplicación analizada	142
Vulnerabilidades encontradas y su mitigación	142
Recursos interesantes	147