EUROPUB JOURNAL OF MULTIDISCIPLINARY RESEARCH
Europub European Publications
ISSN: 2795-4587

DOI: 10.55033/ejmrv4n1-002

Recebimento dos originais: 26/05/2023
Aceitação para publicação: 26/06/2023

Consideraciones de seguridad para el comercio electrónico en dispositivos móviles inteligentes

Considerações de segurança para o comércio eletrônico em dispositivos móveis inteligentes

Diego Arturo Ponce Vásquez
Doctor en Ingenieria Telematica
Institución: Universidad Politecnica de Cataluña (UPC)
Dirección: Carrer de Jordi Girona, 31, 08034 Barcelona, España
Correo electrónico: diego.ponce@ucuenca.edu.ec

Ritha Mireya Cedeño Luna
Master en Dirección de Gestión Estratégica de Información y el Conocimiento en las Organizaciones
Institución: Universidad Abierta de Cataluña (UOC)
Dirección: Rambla del Poblenou, 156, 08018, Barcelona, España
Correo electrónico: ritha.cedeno@ucuenca.ec

RESUMEN
El comercio electrónico en entornos móviles tiene más de tres décadas de investigación y desarrollo. Sin embargo, los cambios tecnológicos hacia redes de telecomunicaciones de 5G y las plataformas de computación en la nube plantean nuevos retos y oportunidades. Este artículo aborda desde una perspectiva histórica los principios de diseño más relevantes, las vulnerabilidades, riesgos, amenazas y las oportunidades, así también los criterios para la implementación cuidadosa de aplicaciones seguras y robustas, al final del artículo se presenta una propuesta de seguridad en este entorno.

Palabras clave: comercio electrónico móvil, m-commerce, ciberseguridad, computación móvil en la nube.

RESUMO
O comércio eletrônico em ambientes móveis tem mais de três décadas de pesquisa e desenvolvimento. No entanto, as mudanças tecnológicas em direção às redes de telecomunicações 5G e às plataformas de computação em nuvem apresentam novos desafios e oportunidades. Este artigo aborda, a partir de uma perspectiva histórica, os princípios de design mais relevantes, as vulnerabilidades, os riscos, as ameaças e as oportunidades, bem como os critérios para a implementação cuidadosa de aplicativos seguros e robustos, e uma proposta para a segurança nesse ambiente é apresentada no final do artigo.

Palavras-chave: comércio eletrônico móvel, m-commerce, segurança cibernética, computação em nuvem móvel.

EUROPUB JOURNAL OF MULTIDISCIPLINARY RESEARCH
Europub European Publications
ISSN: 2795-4587

1 INTRODUCCIÓN

El comercio electrónico en entornos inalámbricos y especialmente de telefonía móvil celular, denominado m-Commerce puede definirse, en términos generales, como cualquier transacción financiera o comercial con intercambio de información que se realiza sobre redes de comunicación de datos en que existe movilidad del usuario. El exitoso despliegue de la telefonía móvil y celular a nivel mundial ofrece una importante oportunidad para la expansión del comercio electrónico sobre este entorno y tiene las siguientes características: a) Disponibilidad de negocios y servicios en la vecindad del cliente, b) Acceso inmediato y georreferenciado para el usuario móvil, c) Posibilidad de completar la transacción en forma inmediata, en cualquier momento y desde cualquier lugar y d) transacciones de diferente cuantía con mecanismos electrónicos de pago [1]. En este artículo se hace un recuento de la evolución tecnológica y de la seguridad para este entorno, se enumeran las recomendaciones para el usuario en cuanto a la protección de sus datos, se presentan las recomendaciones para el desarrollo de aplicaciones web seguras, se reflexiona sobre el marco regulatorio y sus problemas, luego se aborda el tema de la formación en ciberseguridad y las perspectivas de futuro, se presenta una propuesta de seguridad en este ambiente de telefonía móvil inteligente y se finaliza con las conclusiones.

2 CARACTERÍSTICAS DEL ENTORNO

El comercio electrónico en entornos de telefonía móvil celular lleva más de tres décadas de investigación y desarrollo, tuvo sus inicios adaptando las mejores prácticas de Internet a los entornos móviles de naturaleza inherentemente inalámbrica, típicamente los dispositivos de telefonía móvil celular contrastados con los entornos de computación personal se caracterizaban en su inicio por una limitada capacidad de procesamiento de datos, menores anchos de banda, ruido y desconexión impredecible, limitaciones de energía y menor facilidad de uso. Afortunadamente las limitaciones que fuesen identificadas en los inicios de este entorno van siendo superadas por los

EUROPUB JOURNAL OF MULTIDISCIPLINARY RESEARCH
Europub European Publications
ISSN: 2795-4587

cambios de generación tecnológica de telefonía móvil celular, hoy disponemos de mejores anchos de banda, posibilidad de conmutar de red de telefonía móvil y celular a redes wifi y bluetooth, conexión USB, mejor formato de pantalla, entorno táctil y mejor capacidad en el procesador y en memoria, todos estos esenciales para soportar mecanismos y protocolos de seguridad criptográfica para la protección de los datos.

El despliegue de la telefonía móvil celular se ha dado en forma vertiginosa más que el mismo Internet, se pronostica que los teléfonos móviles inteligentes representarán el 80% del tráfico móvil total en el año 2020, comparado con el 76% que se generó en el 2015 [2]. Del lado del servidor también se ha producido una importante evolución hacia la computación en la nube con un impacto sobre la infraestructura, la plataforma y los servicios, hoy nos desenvolvemos en un entorno de clientes móviles conectados a servicios de computación en la nube, entornos en los que buscamos realizar transacciones de forma segura, su diseño e implementación impone algunos retos entre ellos la creciente complejidad de las plataformas de cuarta y quinta generación.

Un aspecto a tener en cuenta en los teléfonos móviles inteligentes es el sistema operativo que abre y pone a disposición de la aplicación de software el micrófono, la cámara, GPS y la información de sensores y archivos en general sin las restricciones y el control de usuario que proveen los S.O. de computadores personales. Existen al día de hoy vulnerabilidades en las máquinas virtuales de Java, en los sistemas operativos y en el control de acceso a los recursos del usuario.

Los abusos van desde el uso hecho por el malware para monitorear sensores tales como GPS, micrófono, sistema de archivos, accediendo a información privada del Smartphone tanto de uso personal como empresarial en el mismo aparato, luego se utiliza esa información para exponerla públicamente, para robar al usuario y a su empresa, y para espiar sus movimientos, esto lo expone a publicidad no deseada, spam, hackeo de datos confidenciales y otros perjuicios.

EUROPUB JOURNAL OF MULTIDISCIPLINARY RESEARCH
Europub European Publications
ISSN: 2795-4587

Entre los requerimientos para las plataformas de teléfonos móviles inteligentes se encuentran: a) la seguridad para el sistema operativo específico, b) herramientas de análisis de seguridad, c) coordinación de protección contra vulnerabilidades, d) permisos para aplicaciones y lenguajes, e) aplicaciones híbridas web/mobile con brechas de seguridad específicas en el entorno móvil, f) ciber higiene en cuanto al uso a la defensiva de parte del usuario, g) uso de mecanismos de cifrado tanto en el sistema de archivos como en canal de comunicación y h) protección en la banda base.

Se han de discriminar dos dominios; el uno en cuanto a las aplicaciones que operan en el teléfono móvil inteligente y por otra parte los privilegios y permisos para acceder a los datos dentro del dispositivo [11].

2.1 EVOLUCIÓN TECNOLÓGICA Y SEGURIDAD

Durante la década de los años ochenta, se establecen los principios que guiaron el diseño de sistemas computacionales, uno de ellos es el principio de diseño extremo a extremo cuyos autores establecen los criterios para el diseño cuidadoso de aplicaciones en entornos complejos [3]. Se analiza la necesidad de implementar en los extremos de la comunicación las aplicaciones de detección y corrección de errores en las capas altas de los protocolos de aplicación o mejor en cada extremo de la comunicación. Una importante aplicación de este principio es de la comunicación cifrada de datos: si el sistema de transmisión de datos realiza el cifrado y descifrado de datos, primero se ha de confiar en la gestión segura de las claves de cifrado/descifrado, en segundo lugar; los datos estarán en claro y por consiguiente vulnerables mientras pasan del nodo destino hacia la aplicación de destino. En tercer lugar, la autenticidad del mensaje se debe verificar siempre en la aplicación. Si la aplicación realiza el cifrado de extremo a extremo y obtiene la autentificación, puede gestionar las claves a su satisfacción y los datos no quedan expuesto fuera de la aplicación, por consiguiente no se necesita que el subsistema de comunicación provea cifrado automático de todo el tráfico, aunque puede ser necesario para asegurar que la aplicación no tenga un comportamiento anómalo al transmitir

EUROPUB JOURNAL OF MULTIDISCIPLINARY RESEARCH
Europub European Publications
ISSN: 2795-4587

deliberadamente información que no debería quedar expuesta, en este último caso se utilizaría cifrado y descifrado en las capas altas y también en las capas bajas del protocolo de comunicación en forma automática, de todas formas hay riesgo en la gestión de claves y otros parámetros de la comunicación por lo que la comunicación no sería completamente segura, por ejemplo: en la pasarela entre red fija y red móvil, aún así la protección de los datos y credenciales almacenadas en el mismo teléfono inteligente son también vulnerables.

La red GSM, red de segunda generación 2G, se diseñó durante los años ochenta cuando aún existía la guerra fría. Debido a la presión política de los gobiernos europeos, se hizo la seguridad de GSM deliberadamente débil para facilitar por ley la interceptación por parte de las agencias. La seguridad se fortaleció en las tecnologías de móviles nuevas de 3G y 4G, la débil seguridad heredada de la segunda generación representa el "eslabón más débil de la cadena" y consiguientemente debilita la seguridad de la red en su totalidad. Por otra parte, las redes inalámbricas Wifi también han tenido su evolución en cuanto a proveer mejores mecanismos de seguridad. Mientras pervivan los sistemas de 2G y las comunicaciones Wifi mantengan protocolos antiguos como WEP persistirá esta debilidad en cuanto a la seguridad [5].

Cuando nos centramos en el tema de seguridad hemos de tener en cuenta que el presente es consecuencia del pasado, los riesgos de los teléfonos móviles inteligentes actuales se han incrementado [4]. Hoy los teléfonos móviles inteligentes con capacidades avanzadas comparables a las que tienen las computadoras personales están disponibles en los bolsillos, carteras y maletines de todo el mundo, su popularidad y seguridad relativamente laxa los han convertido en un objetivo atractivo para los atacantes. Lo que es peor, los atacantes utilizan una combinación de nuevas y viejas técnicas con una creciente variedad y sofisticación en los ataques, muchas veces las contramedidas llegan al mercado lentamente en comparación con el ritmo de los ataques. Típicamente los teléfonos móviles inteligentes proveen a sus usuarios acceso al correo electrónico, el internet, navegación GPS, redes sociales y otras aplicaciones. En los entornos de telefonía móvil celular no funcionan bien medidas de seguridad

EUROPUB JOURNAL OF MULTIDISCIPLINARY RESEARCH
Europub European Publications
ISSN: 2795-4587

tales como cortafuegos, antivirus, y mecanismos de cifrado, sus sistemas operativos y aplicaciones no se actualizan con la misma frecuencia que los computadores personales. Otro problema son las aplicaciones, por ejemplo, las redes sociales carecen de controles detallados de privacidad existentes en su contraparte de computadores personales. Los usuarios cada día incrementan más y más sus actividades y a menudo almacenan en sus teléfonos información sensible, correos personales, calendarios, información de sus contactos, contraseñas y generalmente desconocen o no son capaces de aprovechar el software de seguridad que viene con su aparato, incluso suelen tener la falsa percepción de que navegar desde sus teléfonos celulares es más seguro que desde sus computadores personales, otras veces por la prisa toman atajos dejando de lado la protección de sus información. Recientes innovaciones en comercio electrónico móvil permiten a sus usuarios conducir muchas transacciones desde su teléfono inteligente tales como la compra de bienes y aplicaciones sobre redes inalámbricas, cupones de descuento y tickets, banca en línea, procesamiento de pagos en puntos de venta, e incluso pago en máquinas registradoras y dispensadores de productos.

Los ataques típicos se elevan de la portabilidad a la semejanza con los ataques a los computadores personales, lo que deja abierto un rango de ataques que pueden ir desde el robo del aparato telefónico con la consiguiente pérdida de la información que reside en el dispositivo, lo que incluye información corporativa y financiera, tal que un hacker con suficiente tiempo y las habilidades podría romper el acceso a esta información residente en el teléfono. Las aplicaciones aparentemente legales que se instalan en los teléfonos móviles pueden ser maliciosas, el malware puede distribuirse desde proveedores de tercera parte sin ningún control ni evaluación de seguridad, accediendo incluso a información normalmente bloqueada, saltándose los mecanismos de los sistemas operativos una vez se han instalado estas aplicaciones, incluso las aplicaciones legítimas pueden presentar brechas de seguridad en su código que pueden ser explotadas para espiar, colapsar el software o conducir otros tipos de ataque, por ejemplo; el solo hecho de hacer “click” en un vínculo a otro sitio

EUROPUB JOURNAL OF MULTIDISCIPLINARY RESEARCH
Europub European Publications
ISSN: 2795-4587

web en el navegador. El “pishing”, la combinación engañosa de teclas y “clicks” que conducen a la instalación de una aplicación maliciosa, el “vishing” equivalente del “pishing” con voz, y el “smishing” que consiste en el envío de mensajes cortos tipo SMS y MMS, cargos y pagos fraudulentos en su cuenta, peticiones dolosas de donaciones para la caridad, spam, bullying y otras.

Las consecuencias de los ataques a dispositivos móviles pueden ser severas, los hackers tienen herramientas que pueden convertir a un dispositivo móvil en un robot de red “Botnet” desde el que perpetrar un ataque a otros, pueden difundir virus por la red y ejecutar comandos peligrosos desde el sistema operativo del teléfono, acceder a cuentas y tarjetas de crédito, extraer información personal, acceder a los servicios en línea del usuario, sus identificaciones de usuario y contraseña, y todo lo necesario para tomar control con la información del usuario tales como contactos y localización GPS por ejemplo; para un secuestro. Otro tipo de ataque en el que se bloquea el teléfono y se extorsiona para desbloquearlo se denomina “Ransoming”.

2.2 RECOMENDACIONES AL USUARIO PARA LA PROTECCIÓN DE SU TELÉFONO MÓVIL

Mientras los teléfonos móviles inteligentes evolucionan hacia capacidades similares a los computadores personales, hay una falta de soluciones de seguridad si lo comparamos con los entornos de computación personal, ante este escenario se hacen las siguientes recomendaciones de seguridad:

a) Considere las características de seguridad al momento de comprar un teléfono móvil inteligente, que incluya facilidades de cifrado criptográfico, autentificación, cifrado de los datos residentes en el teléfono y respaldo cifrado de datos. Si va a utilizar red privada virtual utilice certificados digitales y protección de contraseñas, acceso remoto para borrado.

b) Configure el dispositivo para incrementar el nivel de seguridad, por ejemplo; con bloqueo de contraseña o PIN incorrectos, bloqueo del reseteo de su aparato e instale antivirus, antispyware y anti malware.

EUROPUB JOURNAL OF MULTIDISCIPLINARY RESEARCH
Europub European Publications
ISSN: 2795-4587

c) Configure su navegador web para utilizar conexiones seguras, utilice protocolo HTTPS, SSL, WTLS como protocolo de protección de sus sesiones web y redes sociales.

d) No siga vínculos web, no abra correos o mensajes de texto sospechosos.

e) Limite la exposición de su número telefónico celular.

f) Considere cuidadosamente que información va a almacenar en su teléfono móvil celular.

g) Mantenga control del acceso físico a su teléfono móvil, especialmente en espacios públicos.

h) Desactive Bluetooth, Infrarrojo o Wifi cuando no los use.

i) Configurar Bluetooth en modo incógnito para que no lo descubran sin su consentimiento.

j) Evite conectar con redes wifi desconocidas.

k) Borre toda su información antes de descartar un teléfono viejo.

l) Al instalar aplicaciones no permita el acceso a la raíz o “root” ni “jailbreak” de su sistema operativo, limite los privilegios de acceso al momento de instalar una aplicación.

En caso de robo, actúe rápidamente:

a) Reporte la pérdida de su teléfono al proveedor del servicio y a su organización.

b) Cambie sus credenciales de acceso a la información, su administrador de servicios le ayudará.

c) Si su teléfono tiene borrado remoto utilícelo para borrar todos sus datos del teléfono. [4]

2.3 CONSIDERACIONES DE SEGURIDAD PARA EL DESARROLLO DE APLICACIONES WEB SEGURAS

En un entorno de la complejidad de Internet, con la infraestructura como servicio, con usuarios conectados mediante dispositivos móviles inteligentes, el desarrollo de aplicaciones seguras, robustas y confiables es todo un reto.

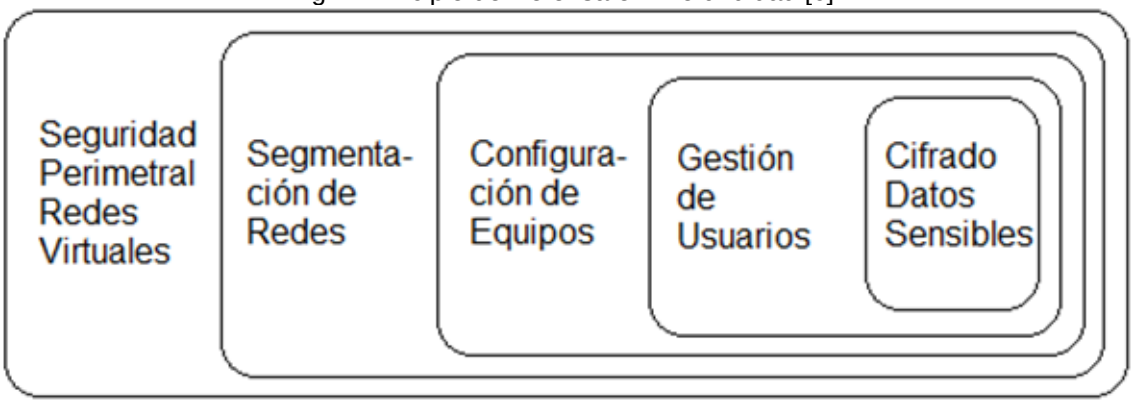
EUROPUB JOURNAL OF MULTIDISCIPLINARY RESEARCH
Europub European Publications
ISSN: 2795-4587

Algunos criterios sin embargo guían el cuidadoso desarrollo de aplicaciones web que operarán en este entorno y se exponen a continuación:

2.3.1 Principio de defensa en profundidad

El principio de defensa en profundidad adopta una filosofía análoga a la defensa de perímetros tal como se ilustra en la figura 1 [6].

Fig 1. Principio de Defensa en Profundidad [6].



Entre las recomendaciones se incluyen en forma concisa las siguientes:

a) Adoptar mecanismos de protección en distintas capas del modelo OSI.

b) Utilizar componentes de software confiables.

c) Sistemas de autentificación, autorización y auditoría (AAA).

d) Infraestructura de clave pública (PKI) y certificados digitales.

e) No ofrecer información de interés a posibles atacantes, tales como mensajes de error, documentación del código, archivos de prueba, entre otros.

El desarrollo de aplicaciones Web seguras refiere a:

a) El código de la aplicación en cuanto a codificación segura.

b) El paso de parámetros de la transacción en URL, Scripts, métodos de HTTP, protocolos de seguridad SSL.

c) La distribución del procesamiento computacional, es decir, qué parte procesa el servidor y que parte el cliente.

d) El control de la transacción; completación y control de réplicas.

e) La gestión de los usuarios: AAA.

EUROPUB JOURNAL OF MULTIDISCIPLINARY RESEARCH
Europub European Publications
ISSN: 2795-4587

f) Verificación de las partes.CD, PKI, TTP.

Recomendaciones de seguridad para comercio electrónico

a) Protección de la transmisión de datos de mediante protocolos de seguridad tales como Kerberos, S/MIME, PGP, WTLS, VPN.

b) Autentificación del usuario: basada en información obtenida del dispositivo y combinada con información solo conocida por el propietario.

c) Aislamiento o “compartimentalización”, es decir, aislar el acceso entre aplicaciones así como entre aplicación y datos.

d) Cifrado de datos sensibles residente en el dispositivo smartphone.

Recomendaciones de seguridad para personas con discapacidad

a) De todas las discapacidades la discapacidad visual es quizás una de las más severas. Posiblemente se deba pensar es dispositivos especialmente diseñados para soportar comandos de voz.

b) En el caso de discapacidad intelectual se debe pensar en dispositivos y mecanismos de pago adaptados de tal manera que garanticen que su uso sea seguro para evitar que el propietario sea abusado. Una medida eficaz suele ser el control del gasto y la posibilidad de gasto de emergencia por ejemplo: para utilizar transporte público.

2.3.2 Aplicaciones Web seguras

Las aplicaciones web han de ser seguras, robustas y resistentes a entornos riesgosos tales como Internet, el entorno en que se ejecutan estas aplicaciones tiene las siguientes características:

Del lado del cliente:

a) Variedad de lenguajes de aplicación.

b) Tipos de clientes: ingenuos, mal informados y maliciosos.

c) El navegador no es confiable.

d) Todo lo que llega del navegador debe filtrarse y verificarse por el servidor.

e) El contenido descargado en el navegador puede editarse con un simple procesador de texto.

EUROPUB JOURNAL OF MULTIDISCIPLINARY RESEARCH
Europub European Publications
ISSN: 2795-4587

f) Se pueden interceptar y modificar los datos enviados desde el navegador al servidor web: cabeceras http, valores en los cookies, …

Del medio de transmisión:

a) Internet es un entorno hostil

b) Protección de injerencia hacker internacional utilizando nuestro propio desarrollo, por ejemplo: utilización de lenguas ancestrales.

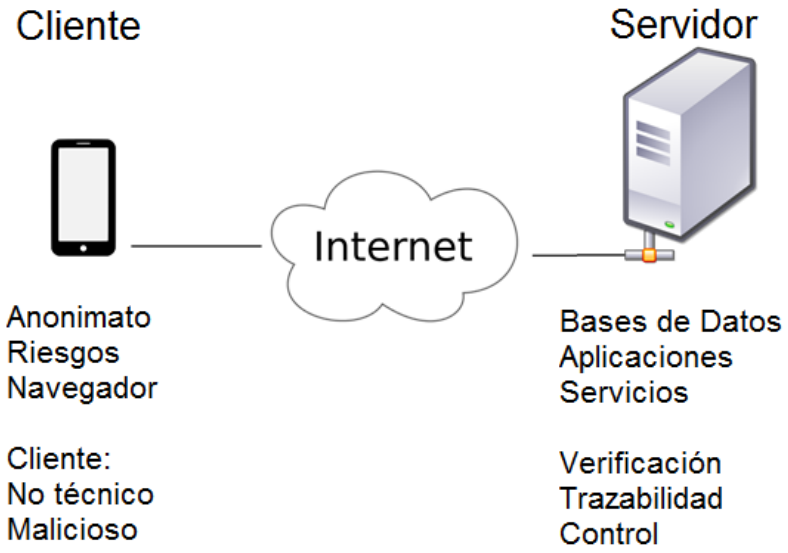
Del lado del Servidor:

a) Validación del lado del servidor

b) Control de parámetros de paso entre sitios (Cross-site scripting)

La figura 2 ilustra este entorno:

Fig. 2. Características del Entorno Cliente-Servidor con Usuarios Móviles.



2.3.3 Recomendaciones para desarrolladores y proveedores de servicio

Entre las recomendaciones básicas para desarrolladores de software que ha de funcionar en entornos Web se deben hacer las siguientes consideraciones respecto de la arquitectura, entorno, principios y actividades de desarrollo.

Arquitectura en tres niveles:

a) Interfaz de cliente

b) Reglas de negocio

c) Acceso a datos / BD.

d) Validación y Autentificación:

EUROPUB JOURNAL OF MULTIDISCIPLINARY RESEARCH
Europub European Publications
ISSN: 2795-4587

e) Puesto que el entorno no es seguro estas funciones debe realizarlas el lado del servidor.

f) Existen los mecanismos y protocolos de seguridad para proteger la información.

Principios fundamentales y recomendaciones básicas:

a) Seguridad extremo a extremo

b) Defensa en profundidad

c) Validación del Código

Actividades para el desarrollo seguro de aplicaciones:

a) Protección de la informacion transmitida

b) Autenticación del usuario.

c) Control del entorno, privilegios, pruebas de seguridad.

d) Validación de entrada /salida de datos en las aplicaciones.

e) Control de la Interacción entre el cliente y el servidor web.

f) Otros: equipos intermedios, hosting y housing.

g) Los mecanismos deben ser lo más amigables para los usuarios.

Los propios programadores y analistas deben usar:

a) Un entorno seguro.

b) Un lenguaje que facilite la codificación Web segura.

c) Someter la aplicación a pruebas de seguridad.

Validación:

a) Validar el diseño inicial en papel.

b) Utilizar analizadores de código fuente para detectar errores lógicos y de codificación.

c) Utilizar herramientas de análisis de vulnerabilidades.

d) Diseñar casos de prueba para verificar la aplicación.

e) Validar la interfaz de usuario.

f) Contratar auditorías de seguridad.

EUROPUB JOURNAL OF MULTIDISCIPLINARY RESEARCH
Europub European Publications
ISSN: 2795-4587

2.3.4 El código

Contrario a la buenas prácticas de desarrollo de software en las que un código claro, suficientemente explicado, comentado y documentado era la practica ética, en entornos hostiles como el Internet el desarrollo del software en general enfrenta dos problemas: la ofuscación general del software y la ofuscación criptográfica.

La ofuscación general del software apunta a hacer del software ejecutable tan ininteligible como sea posible, tal que un adversario tenga problemas en entender la lógica del programa, y esto se logra con la transformación del léxico, transformación del control y transformación de los datos.

La ofuscación criptográfica por otro lado busca ocultar las claves secretas empotradas en el software, por ejemplo mediante el uso de una función de hash que oculte la entrada de una determinada función de software, si es lo suficientemente fuerte puede servir para el cifrado homomórfico. Tanto uno como otro tipo de ofuscación sirven en la práctica. Ejemplos de su utilidad puede ser el ocultamiento del código de verificación de licencia de software, deshabilitar características cuando se salta el proceso de validación de claves, y otras más.

El objetivo final es convertir al software en una caja negra virtual, otra propiedad de indistinguibilidad evitando dar pistas que conduzcan a la rotura de claves, por ejemplo; con el tiempo de ejecución de una determinada aplicación de validación tal que permita deducir el tamaño de una clave por medios matemáticos o de análisis del software [7].

Eliminar de los directorios accesibles desde la Web:

a) Comentarios de los archivos HTML.

b) Archivos de prueba.

c) Copias de seguridad.

d) Archivos no utilizados.

Limitar la información en el código que recibe el Cliente (scripts).

a) Eliminar la información de error.

b) Controlar la información en la aplicación que se muestra al usuario.

c) Archivo Index.html en cada directorio web.

EUROPUB JOURNAL OF MULTIDISCIPLINARY RESEARCH
Europub European Publications
ISSN: 2795-4587

El aislamiento y la interacción de aplicaciones en los sistemas operativos de los dispositivos móviles inteligentes de hoy en sistemas populares como Android, el diseño de la denominada caja de arena para aplicaciones (application sandbox), el espacio de memoria y el acceso a las áreas protegidas del sistema de archivos no deben interferir con otras aplicaciones vitales para el desempeño de los dispositivos móviles, el aislamiento debe ser tal que las aplicaciones de malware no puedan explotar una brecha de seguridad [8][10].

3 ESTADO DEL MARCO REGULATORIO

El marco regulatorio se enfrenta a problemas tales como la dificultad de lograr regulaciones transfronterizas, problemas con la delimitación de la responsabilidad en una plataforma abierta al mundo, sin embargo, todos coincidimos en la necesidad de regulación, información, penalización y concienciación. Esto es un tema especialmente delicado cuando se trata de las agencias de seguridad en el mundo quienes pueden solicitar se rebaje la protección criptográfica para poder intervenir las comunicaciones por diferentes razones, quedando la privacidad de las comunicaciones como un tema delicado de debate. En el Ecuador existen varios esfuerzos, los más destacados en el sector público podemos citar a ECUCERT y el Comando de Ciberdefensa de las Fuerzas armadas de Ecuador.

En el campo normativo son las normas ISO 27000, 31000, 37000, el proyecto OWASP, COBIT, ITIL e-TOM, estándares que engloban las buenas prácticas.

4 FORMACIÓN Y FUTURO

El siguiente paso de los computadores personales a los teléfonos móviles inteligentes será la conexión entre el mundo digital y el mundo físico, la posibilidad de comandar drones desde los dispositivos móviles así como el emergente internet de las cosas que integrará un conjunto básico de sensores fusionando el procesamiento computacional con sistemas de GPS, acelerómetros, magnetómetros, comunicación por Internet suficiente para

EUROPUB JOURNAL OF MULTIDISCIPLINARY RESEARCH
Europub European Publications
ISSN: 2795-4587

mantener una investigación y desarrollo para las décadas siguientes. Los drones incorporan actuadores y propulsión propia, miembros artificiales para interactuar con su entorno una fusión de computación, sensores y actuación combinados con un desarrollo en la teoría de robots autónomos lograran otro tipo de interacciones con el entorno en una mezcla de humanos, drones y teléfonos móviles inteligentes. La interacción impone sus propios retos entre actuación guiada y actuación autónoma de los drones en entornos tridimensionales. Su desarrollo se lleva en una amplia gama de artefactos desde juguetes hasta aplicaciones militares. Sin duda esto también impone una serie de retos éticos, de ciberseguridad vehicular y vigilancia del espacio aéreo [9].

De especial mención son la recomendación de malla curricular de ACM/IEEE CS'2013. Al momento de la formación un profundo conocimiento de los conceptos teóricos sobre los que subyacen los diferentes mecanismos de seguridad y la necesidad de desarrollo de nuestras propias soluciones, así también en la formación de nuevos profesionales. Sigue siendo un reto formar un profesional diestro que conozca la diferencia entre certificarse y ser capaz de afrontar situaciones reales, en definitiva que conozca los patrones y antipatrones de seguridad en este entorno.

5 COMPUTACIÓN EN LA NUBE

Las arquitecturas de computación en la nube esconden la complejidad, alta disponibilidad, redundancia, virtualización y aplicaciones en un entorno distribuido y difuso de donde nos llegan los servicios, pero de los que poco sabemos respecto de su seguridad. La complejidad de esta plataforma puede esconder brechas de seguridad fácilmente, de modo que lo que se gana en cuanto a las prestaciones de esta plataforma se puede perder en cuanto al control que tenemos del tema de seguridad de nuestros sistemas y servicios.

6 PROPUESTA DE SEGURIDAD EN TELÉFONOS MÓVILES INTELIGENTES

Un teléfono móvil inteligente, para los fines prácticos debería considerar un diseño de seguridad similar al de un computador personal, existe un criterio

EUROPUB JOURNAL OF MULTIDISCIPLINARY RESEARCH
Europub European Publications
ISSN: 2795-4587

minimalista que dice que menos es más, y esto cuenta en entornos que todavía tiene restricciones tales como consumo de energía, capacidad de procesamiento menor, posibilidad de funcionar en línea y fuera de línea, posibilidad de interactuar a través de diferentes canales inalámbricos tales como USB, Bluetooth, Wifi y la red móvil Celular. Una propuesta de seguridad debe necesariamente cubrir los siguientes aspectos:

a) Análisis de autorización de acceso al usuario del dispositivo móvil inteligente.

b) Permisos de acceso en las carpetas y archivos del dispositivo.

c) Permisos de las aplicaciones que se ejecutan en el dispositivo.

d) Aislamiento entre aplicaciones para evitar la colusión fraudulenta.

e) Escaneo de malware.

f) Advertencia al usuario.

g) Consejero de seguridad en el dispositivo.

h) Detección de intrusiones y protección contra intrusiones.

i) Perímetros de seguridad.

j) Autentificación del canal inalámbrico.

k) Control del acceso remoto a los recursos del dispositivo.

l) Detección de actividad no usual.

Para cubrir estos aspectos en un dispositivo que se encuentra siempre conectado, hace falta actualización y diagnóstico en línea, esto genera una sobrecarga (overhead) en el canal de comunicación.

Otras amenazas son el “ransomware” y los ataques de día cero, la detección de “exploits” y su cura, la suplantación de identidad y el acceso a mecanismos de pago, se ha de considerar también la sustracción del aparato. La solución debería contener al menos estos mecanismos:

a) Un IDS e IPS para smartphones capaz de enfrentar varios de estas restricciones.

b) Un sistema de análisis de vulnerabilidades en línea accesible al usuario y con posibilidades de autentificación y diagnóstico confidencial.

EUROPUB JOURNAL OF MULTIDISCIPLINARY RESEARCH
Europub European Publications
ISSN: 2795-4587

c) Un cortafuego que “compartimentalice” es decir, aísle las aplicaciones y separe los perímetros con un criterio de defensa en profundidad.

d) Protección de credenciales, es decir, autentificación y autorización de usuarios.

e) Posibilitar en bloqueo y formateo en caso de robo.

Los ataques de hoy son ataques basados en herramientas inteligentes, los virus cifran su código, comprimen su archivo, mutan el código, haciéndolos de esta manera polimórficos, mutantes, y como consecuencia irreconocibles por los sistemas de antivirus. Teniendo en cuenta que el usuario no es capaz de manejar por su cuenta la complejidad de este entorno, que también podría tratarse de un usuario malicioso y aún peor: el entorno reúne los riesgos y vulnerabilidades del entorno inalámbrico, del sistema operativo, de las aplicaciones que funcionan en el dispositivo, de la falta de aislamiento de entre datos sensibles y aplicaciones, de control de los permisos y privilegios del usuario y de las aplicaciones, en definitiva de todas las vulnerabilidades de varias generaciones de telefonía móvil celular a la que se suman las vulnerabilidades de los computadores personales, esto exige de los fabricantes una nueva generación de herramientas de detección y protección, capaces de manejar las vulnerabilidades del entorno, dotadas de inteligencia artificial para evaluar cualquier comportamiento anómalo del dispositivo y con capacidad de protección automatizada ante cualquier eventualidad, todo esto en un entorno en donde hay limitaciones de energía, procesador y memoria, combinados con un canal inalámbrico con múltiples tecnologías, se convierte en el entorno más difícil, retador e inseguro que ha existido en los últimos tiempos.

7 CONCLUSIONES

La complejidad de los servicios geolocalizados en la vecindad del usuario con disponibilidad inmediata en una red pública de telefonía móvil celular hace de este entorno especialmente vulnerable si se considera el desconocimiento del usuario y la falta de disponibilidad de herramientas de seguridad inteligentes para este tipo de entorno.

EUROPUB JOURNAL OF MULTIDISCIPLINARY RESEARCH
Europub European Publications
ISSN: 2795-4587

El desarrollo de aplicaciones web seguras en producción requiere un conocimiento profundo de los métodos y herramientas, así como los fundamentos de diseño, teoría de números y criptografía y conciencia del entorno en el que van a funcionar.

La compatibilidad con un entorno del que hereda características y problemas sin resolver de generaciones tecnológicas anteriores con las que ha de coexistir, y que constituyen el “eslabón débil de la cadena” nos hacen repensar los criterios de diseño tales como el argumento de diseño extremo a extremo, el principio de defensa en profundidad, el desarrollo web seguro y la ofuscación del código, las pruebas de validez, la codificación segura para aplicaciones de software y la seguridad de todo el sistema en conjunto y de cada una de sus partes.

La necesidad de mecanismos de seguridad inteligentes, más eficientes y de fácil configuración que estén disponibles para el usuario en el teléfono móvil inteligente.

La perspectiva de futuro en que los teléfonos móviles inteligentes tendrá posibilidad de interacción con autómatas formando un círculo entre humanos, teléfonos móviles inteligentes y dispositivos automáticos.

La computación en la nube con sus beneficios puede esconder en la complejidad de su plataforma brechas de seguridad de las que no somos conscientes y posiblemente ni siquiera tenemos control.

EUROPUB JOURNAL OF MULTIDISCIPLINARY RESEARCH
Europub European Publications
ISSN: 2795-4587

REFERENCIAS

1. Soriano M., Ponce D.: A Security and Usability Proposal for Mobile Electronic Commerce, Technology Advances for 3G and Beyond, IEEE Communications Magazine, pp.1-2, (August 2002).

2. Adams A.: Possesing Mobile Devices, IEEE Computing Edge, pp.17-22, (Febrero2016).

3. Saltzer J., Reed D., Clark D.: End to End Arguments in System Design, M.I.T. Laboratory for Computer Science, Revised version of a paper from the Second International Conference on Distributed Computing Systems, Paris, France, pp. 509-512.: Copyright 1981 by The Institute of Electrical and Electronics. (April 8-10, 1981).

4. Ruggiero P., Foote J.: Cyber Threats to Mobile Phones, US CERT, United States Computer Emergency Readiness Team, Carnegie Mellon University, (2011).

5. Jøsang A, Miralabé L, Dallot L.: Vulnerability by Design in Mobile Network Security, University of Oslo, Norway, The Journal of Information Warfare, ISSN 1445-3312, Volume 14, Issue 4, (2015).

6. Gómez Á.: Enciclopedia de la Seguridad Informática, 2da. Edición Actualizada, editorial Alfa omega Ra-Ma, ISBN:978-607-707-181-5 Capítulo 19: 19.2- 19.3 pp. 527-553, (2011).

7. Xu H., Lyu M.: Assesing the computer properties of software obfuscation, IEEE Computing Edge, pp.24-27, (December 2016).

8. Memon A., Anwar A.: Colluding Apps: Tomorrow's Mobile Malware Threat, pp. 31-35, IEEE Computing Edge, (March 2016).

9. Allen R., Pavone M., Schwager M.: Flying Smartphones, When Portable Computing Sprouts Wings, Stanford University, IEEE Computer Society, (January 2017).

10. Stallings W., Brown L.: Computer Security, Editorial Pearson, Capítulo 6: Malicious Software, pp.199-237, ISBN:978-0-13-377392-7, (2015).

11. Flynn L., Klieber W.: Smartphone Security, p. 8-11, IEEE Computing Edge, (Febrero 2016).