Alliance for Financial Inclusion
Bringing smart policies to life

Mobile Financial Services Working Group (MFSWG)

Servicios financieros móviles
Riesgos tecnológicos

La presente nota de orientación fue desarrollada por el Grupo de Trabajo de Servicios Financieros Móviles (MFSWG) de AFI, con el fin de identificar los tipos de riesgos tecnológicos inherentes a los servicios financieros móviles y las estrategias para su gestión.

Nota de orientación No.2
Julio de 2013

Contenido

Al reconocer el potencial de los servicios financieros móviles (SFM), el Grupo de Trabajo de Servicios Financieros Móviles (MFSWG) se creó para brindar una plataforma dentro de la red de AFI para el debate de los formuladores de políticas públicas en cuanto a problemas normativos relacionados con los SFM. El grupo de trabajo promueve el amplio uso de los SFM como solución clave para una mayor inclusión financiera en países emergentes y en desarrollo. El objetivo del grupo es estimular el debate y el aprendizaje entre los formuladores de políticas públicas y promover una mayor coordinación entre los diversos actores de los SFM, tales como los entes reguladores financieros y de telecomunicaciones, así como proveedores bancarios y no bancarios.

Contexto

Los servicios financieros móviles (SFM) ofrecen la posibilidad de una mayor eficiencia y conveniencia en las aplicaciones de pago y también podrían proporcionar una base para iniciativas de inclusión financiera.Sin embargo, para que los SFM puedan cumplir su promesa, los proveedores de servicios y los entes reguladores deben considerar seriamente la seguridad de la plataforma dentro de este nuevo mercado.

Debido a que los modelos de negocio, las necesidades del mercado y la abstención normativa varían entre países, esta nota no establece un único conjunto de políticas adecuado para todos los contextos. En cambio, tiene la intención de ayudar a orientar la formulación de políticas públicas, al identificar los tipos de riesgos tecnológicos que son habituales en los servicios financieros móviles y las estrategias para manejarlos. Por lo tanto, esta nota registra gráficamente el flujo de información en operaciones de SFM, identifica los tipos de riesgos tecnológicos que se aplican a dichos flujos de información, y elabora marcos para la gestión y monitoreo de los riesgos. El objetivo de esta nota es ayudar a que los entes reguladores empiecen a pensar acerca de los riesgos tecnológicos en los SFM de una manera flexible que será útil para la toma de decisiones futuras.

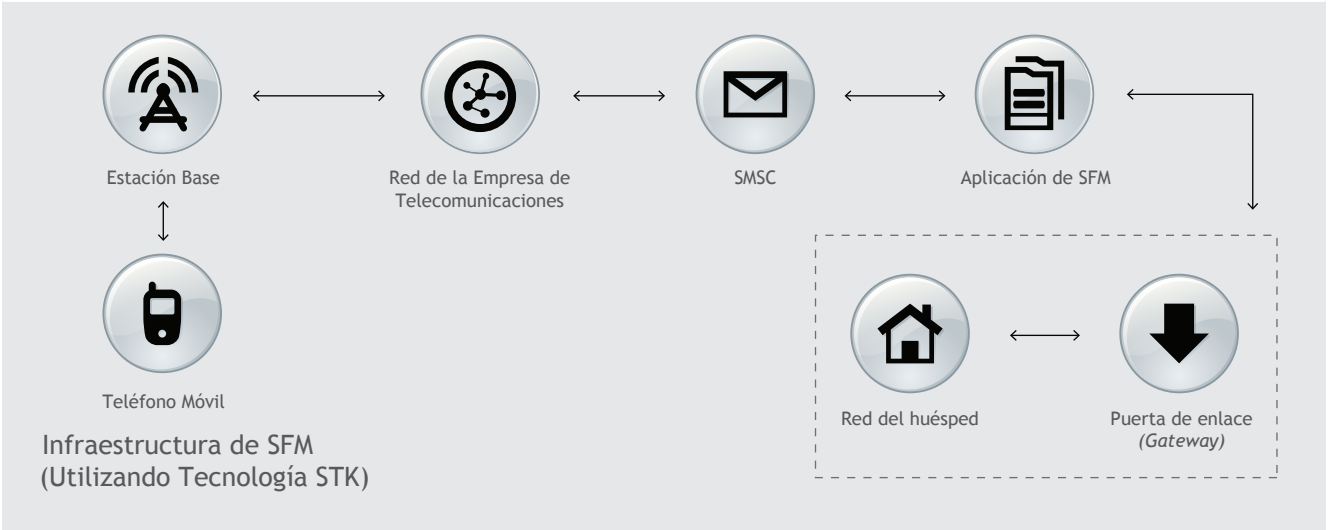
Un comentario acerca del lenguaje: A lo largo de esta nota, se utiliza el término **"amenazas"** para describir las clases de disfunciones en la oferta de SFM y el término **"riesgos"** se refiere a la aplicación de dichas amenazas a los procesos actuales implícitos en una oferta de SFM. En este sentido, los riesgos son casos de amenaza que pueden observarse en operaciones reales.

Flujos de información en SFM

Los entes reguladores necesitan familiarizarse con la forma en que la información fluye dentro de la red de SFM, con el fin de analizar los riesgos tecnológicos que evolucionan en dicho ambiente. Si usted entiende la forma en que cada elemento de la red maneja la información, usted podrá identificar los tipos de controles que se requieren para garantizar la seguridad de dicha información. La Figura 1 es una representación esquemática de dichos flujos de información para SFM basados en la banca que se ofrecen en colaboración con un operador de redes móviles (ORM).

Los usuarios de SFM inician procesos utilizando sus teléfonos. La información proporcionada por cada usuario se envía a la estación base del ORM.[1] En una red GSM, la estación base recibe una solicitud de canal del teléfono móvil y la reenvía al ORM del usuario. En operaciones de SMS, los paquetes de datos que contienen información se procesan en un centro de servicio de mensajes cortos (SMSC, por sus siglas en inglés) y se enrutan al servidor de la aplicación de SFM. A su vez, el servidor de la aplicación de SFM entrega la información de la operación a una puerta de enlace *(gateway)* — la interfaz entre la red del ORM y la red del banco. Entonces, el paquete de datos se somete a una verificación de seguridad y, sujeto a aprobación, se enruta a la red interna del banco para autorización y procesamiento posterior. La red del banco almacena la información financiera y no financiera del usuario y autoriza la operación solicitada por éste. Debido a que este proceso funciona al revés, en este punto el usuario recibe la notificación de que la operación se ha concluido.

Figura 1: Infraestructura de los servicios financieros móviles (utilizando tecnología STK)



[1] Los mensajes enviados por el teléfono tienen un código de identificación que utilizará entonces la estación base para determinar si la red utilizada por el remitente le pertenece. Si es así, el mensaje se reenviará a la red de la empresa de telecomunicaciones. De lo contrario, el mensaje se omitirá. El teléfono continuará buscando una estación base que atienda su solicitud, hasta que haya ocurrido la conexión completa.

Clasificación de amenazas tecnológicas

Resulta importante comprender el flujo de información en operaciones de SFM debido a la variedad de riesgos tecnológicos que están presentes en cada etapa de este flujo. De hecho, resulta útil clasificar los riesgos tecnológicos de acuerdo con su categoría más amplia de amenaza. Dhillon (2007) identifica seis categorías generales de amenazas en los sistemas de información:

Modificación: cuando se tiene acceso no autorizado a la información en el sistema y ésta se cambia sin permiso.

Destrucción: cuando se destruye o pierde el hardware, software, datos o canal de comunicaciones.

Revelación: cuando los datos se ponen a disposición sin el consentimiento del titular.

Interceptación: cuando una persona o software no autorizados obtiene acceso a fuentes de información, permitiendo que programas y otra información confidencial se copie sin autorización.

Interrupción: cuando el servicio o los recursos no están disponibles para su uso, ya sea accidental o intencionalmente.

Fabricación: cuando un usuario no autorizado inserta operaciones falsas en un registro o las agrega a una base de datos.

Este marco de amenazas puede aplicarse al diagrama de proceso de los flujos de información en SFM.

La Figura 2 presenta una visión no exhaustiva de los puntos en los cuales las amenazas pueden introducirse en los flujos de información de SFM.

Tabla 1: Clasificación de amenazas tecnológicas de los SFM

Amenazas	Datos	Software	Hardware	Canal de Comunicaciones
Modificación	Ocurre durante el almacenamiento, transmisión y cambio en el hardware físico	Sucede cuando se altera el software para realizar funciones o cómputos adicionales	–	Ocurre cuando los paquetes se enrutan hacia un destino diferente
Destrucción	Causada por fallas en el hardware y/o software	Destrucción debido a intenciones maliciosas, es decir, software malicioso *(malware)*	Ocasionada por desastres naturales, tales como inundaciones, incendios o por ataques terroristas	Causada por cortes en las líneas de fibra óptica o líneas arrendadas debido a eventos inesperados, es decir, inundaciones, robo o construcción de vías
Revelación	Ocurre cuando hay un acceso no autorizado a los datos/información de otra persona	–	–	–
Interceptación	Sucede cuando usuarios no autorizados reproducen la información confidencial	Ocurre cuando los programas de software se copian en forma ilegítima a partir de una fuente informática	Sucede cuando los usuarios no autorizados obtienen acceso físico al hardware	Ocurre cuando un tercero es capaz de interceptar (escuchar) puertos sin el conocimiento del usuario legítimo
Interrupción	–	Causada por el borrado de programas de software y/o funcionalidades específicas Puede ser el resultado de corrupción en el sistema operativo	Ocasionado por hardware dañado	Causado por ataques maliciosos, tales como saturación y denegación de servicio Puede ser el resultado de desastres naturales, interrupción del suministro eléctrico, problemas con las estaciones base o problemas en la red
Fabricación	Ocasionada por ataques de suplantación de identidad *(phishing)*	–	–	–

Referencia: Dhillon, G. (2007). Principios de seguridad de los sistemas de información: Texto y casos *(Principles of Information Systems Security: Text and Cases)*.

Identificación de riesgos tecnológicos de los SFM

El marco de clasificación que brinda el lenguaje de las amenazas puede ayudarnos a darle sentido a la profusión de riesgos tecnológicos que aquejan a los SFM. Estos riesgos son específicos y variados, pero colocarlos en una ontología de amenazas puede ayudar a organizarlos, evitarlos y eventualmente remediarlos. Este apartado destaca los riesgos específicos y los clasifica de acuerdo con la clase más amplia de amenazas a la que pertenecen.

Amenaza: Modificación

Infección por software malicioso *(malware)* móvil (riesgo)

Los ataques de software malicioso son comunes en el entorno PC y se espera que pronto se extiendan a los dispositivos móviles de manera repentina. Los ataques de software malicioso en teléfonos celulares pueden ocurrir de las siguientes maneras:[2]

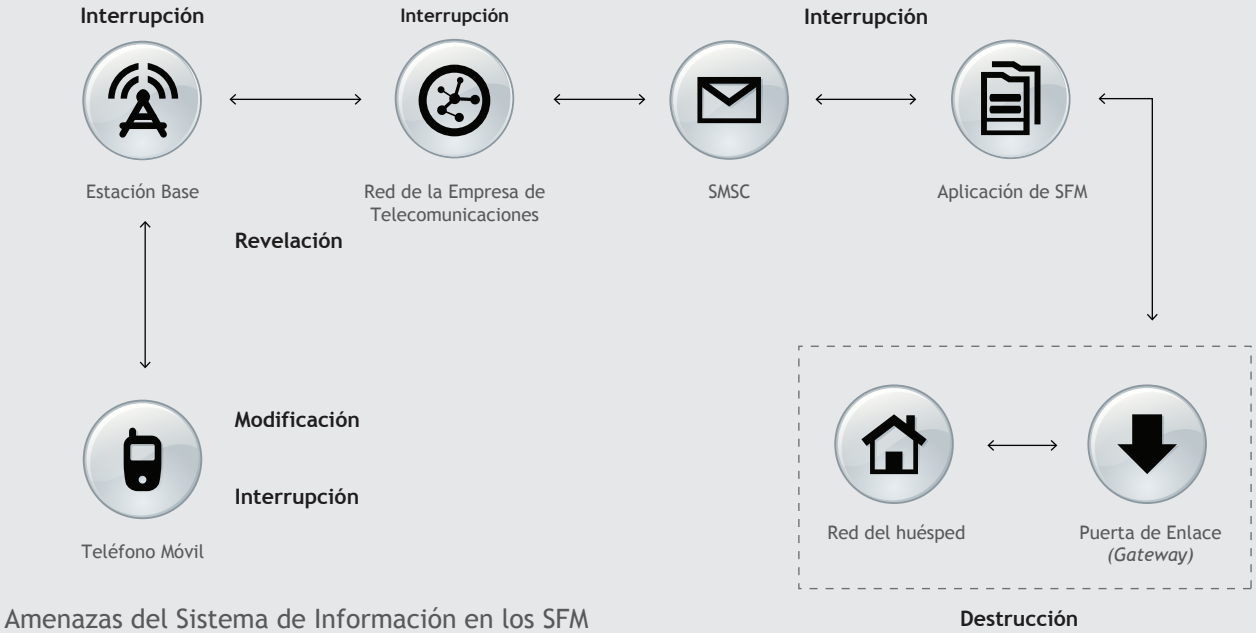
- Los virus/troyanos/gusanos del software malicioso pueden diseminarse vía Bluetooth y MMS.
- El software malicioso puede manipular al usuario al enviar un mensaje SMS.
- El software malicioso puede infectar archivos.
- Los atacantes pueden obtener acceso remoto a los teléfonos celulares al propagar software malicioso.
- Cuando se descarga, el software malicioso puede cambiar los íconos y las aplicaciones del sistema.
- El software malicioso puede instalar funciones y aplicaciones no operativas.
- El software malicioso es un canal útil que puede utilizarse para instalar otros programas maliciosos.
- El software malicioso puede robar datos o información que capture el usuario y bloquear el uso de las tarjetas de memoria.

Amenaza: Revelación

Legibilidad de información financiera crítica de los clientes vía SMS (riesgo)

La legibilidad resulta una gran inquietud cuando se utilizan SMS para tener acceso a cuentas y recibir notificaciones sobre actividades previas. Los SMS se transmiten y reciben en texto simple y dicho protocolo no utiliza ninguna técnica de cifrado. En los casos de robo del dispositivo y software malicioso, los usuarios no autorizados pueden tener acceso total a la cuenta de un cliente.

Figura 2: Amenazas del sistema de información a los SFM



Amenazas del Sistema de Información en los SFM

[2] Gostev, A., 2006.

Amenaza: Revelación

Exposición de datos críticos debido a cifrado no seguro de extremo a extremo (riesgo)

El Protocolo de Aplicaciones Inalámbricas (WAP, por sus siglas en inglés) es una aplicación estándar que permite que los teléfonos móviles tengan acceso a la Internet. Los teléfonos celulares con tecnología WAP utilizan navegadores similares a los que utilizan las computadoras, aunque tienen modificaciones para adecuarse a las restricciones de dichos teléfonos. El WAP utiliza el mismo enfoque estratificado que el TCP-IP. Un sitio web normal basado en la computadora permite a los usuarios tener acceso a la Internet mediante el uso del HTML del protocolo de la capa de aplicación. Asimismo, los consumidores que cuentan con teléfonos móviles con tecnología WAP pueden tener acceso al mismo sitio web utilizando sus teléfonos por medio del protocolo WML (Lenguaje de Marcado Inalámbrico), que es una capa de aplicación del WAP. La única diferencia entre los dos es el tamaño y resolución de la visualización (ya que el sitio web se convierte para atender las restricciones del teléfono móvil). Por lo tanto, las transmisiones no cifradas son vulnerables a quedar expuestas a partes no autorizadas.

Amenaza: Interrupción

Falta de disponibilidad del canal de comunicaciones debido a ataques de denegación de servicio (riesgo)

Los ataques de denegación de servicio (DOS, por sus siglas en inglés) hacen que un recurso computacional no esté disponible mediante la saturación o el consumo del recurso del componente. El objetivo más común de los ataques DOS son los servidores y bases de datos, que también pueden afectar las redes móviles, debido a que tanto el entorno con cables como el inalámbrico utilizan la misma infraestructura.

Amenaza: Interceptación

Ataque por secuencias de comandos entre páginas web *(cross-scripting attack)* en USSD (riesgo)

El protocolo de comunicación USSD permite una transmisión de datos más rápida en comparación con el SMS. A diferencia del SMS, el USSD utiliza una conexión directa entre el remitente y el destinatario. Es un canal de comunicación orientado a la sesión, donde la aplicación USSD se utiliza como interfaz entre el proveedor de telecomunicaciones y la cuenta bancaria del cliente. El USSD también puede manejarse utilizando aplicaciones basadas en la web, por lo que es propenso a ataques por secuencias de comandos entre páginas web. En dichos ataques, un usuario malicioso explota la vulnerabilidad de la aplicación basada en la web instalada en el teléfono móvil del usuario para manipular operaciones (al inyectar una secuencia de comandos Java o SQL a fin de robar la información crítica del usuario). También puede llevar a cabo actos maliciosos en la base de datos, tomar la sesión activa de otro usuario y conectar a usuarios a servidores maliciosos.

La presente lista de riesgos no pretende ser exhaustiva, pero ilustra los tipos de riesgos que cualquier oferta de servicios debe manejar. Tomando en cuenta dichos riesgos, ahora nos abocamos a los principios de la gestión de riesgos y supervisión que los entes reguladores deben conocer.

Riesgos tecnológicos de los SFM: Gestión y monitoreo

PRINCIPIOS

Existen cinco principios clave que sirven de guía para la gestión de riesgos en los SFM: Confidencialidad, Integridad, Disponibilidad, Autenticación e Irrefutabilidad. Cada uno de esos principios se analiza a continuación.

Tabla 2: Modelo del impacto de los riesgos

PROBABILIDAD	IMPACTO				
	Desastroso	Alto	Moderado	Bajo	Insignificante
Casi segura	E	E	E	A	M
Probable	E	E	A	A	M
Posible	E	E	A	M	B
Poco probable	E	A	M	B	B
Rara	A	A	M	B	B

NIVEL DE RIESGO: E= Extremo A= Alto M= Moderado B= Bajo

Confidencialidad: para proteger los datos del usuario de acceso no autorizado o robo. Es importante distinguir entre datos financieros y no financieros, debido a que diferentes principios de confidencialidad se aplican a cada uno de ellos. En general, los datos financieros requieren normas de cifrado más estrictas para su visualización, almacenamiento y transmisión. Los números de identificación personal deben almacenarse en forma cifrada y no estar disponibles para el personal del proveedor del servicio. Fuertes normas de criptografía deben aplicarse a los datos que se transmiten por las redes públicas, tales como la Internet y las redes celulares. Los datos no financieros pueden mantenerse en forma confidencial con medidas un poco menos estrictas, tales como establecer cortafuegos *(firewalls)*, implementar sistemas de prevención y detección de intrusos, y utilizar controles de acceso.

Integridad: la entereza, precisión y confiabilidad de los datos que se presentan. Para validar la integridad de los datos, debe verificarse el proceso que identifica los campos faltantes, llevarse a cabo verificaciones de secuencias y verificarse el resumen criptográfico total[3] así como la longitud variable. La integridad de los datos resulta más importante durante la transmisión, ya que es más probable que la interceptación y manipulación de datos ocurran en esta etapa.

Disponibilidad: los datos y servicios deben ser accesibles cuando los usuarios legítimos deseen utilizar los SFM. Existen diversos escenarios que pueden amenazar la disponibilidad de los datos y servicios. Los riesgos tecnológicos de la disponibilidad del servicio incluyen desastres ambientales (tales como interrupciones del suministro eléctrico, ataques terroristas y causas de fuerza mayor) y actos maliciosos, tales como ataques de denegación de servicio.

Autenticación: establecer la identidad del usuario y del proveedor de servicios.

- Los **usuarios** deben confiar en que el huésped que solicita la conexión está autorizado y que no hay terceros involucrados en la conexión entre la terminal y los servidores huésped. Lo anterior incluye también control de acceso, control de permisos y autenticación de contraseñas.
- Los **proveedores de servicios** deben confiar en que la persona que tiene acceso a los datos es quien dice ser. Los registros de auditoría evalúan la validez y congruencia de los datos que circulan en la red y son herramientas importantes para verificar si los comandos han sido ejecutados por usuarios legítimos. De esta forma, los entes reguladores deben ser capaces de considerar la forma en que los proveedores de servicios monitorean los registros de auditoría. Asimismo, deben establecerse procedimientos y operaciones administrativos para controlar el acceso a la información de los clientes y comprender las vulnerabilidades del sistema.[4]

Irrefutabilidad: la propia protección del proveedor de servicios del posible comportamiento abusivo por parte de los consumidores y empleados, garantizando la conclusión y seguridad de la operación. Asegurarse de que las personas acepten los términos y condiciones del servicio antes de llevar a cabo cualquier acto y utilizar firmas digitales para prevenir que las personas nieguen sus actos. Los certificados de clave pública también permiten a los proveedores de servicios rastrear el origen de la operación en caso de que no haya un intercambio directo de información entre entidades.

Estos principios ofrecen un marco para entender las vulnerabilidades en los SFM, que complementan el debate acerca de las amenazas y riesgos. Considerar las amenazas como infracciones a los principios administrativos claves, puede ayudar a determinar la solución normativa necesaria. El proceso de gestión de riesgos ayuda a formular y calibrar dicha solución más a fondo.

PROCESO

La gestión de riesgos se desarrolla al (1) evaluar los riesgos, (2) analizar dichos riesgos por impacto esperado y probabilidad, y (3) monitorear dichos riesgos de acuerdo con las expectativas y probabilidad del impacto.

1) **Evaluación de riesgos.** Los criterios de evaluación permiten que se analicen a profundidad las posibles amenazas al sistema. Se sugieren los siguientes criterios para los SFM:
   - Viabilidad de la amenaza: ¿Ya ocurrió esta amenaza? ¿Qué elementos se vieron afectados? ¿El software? ¿El canal? ¿Cuánto tiempo pasó antes de que se identificara esta amenaza?
   - Incidentes registrados: ¿Cuántas veces ha ocurrido esta amenaza durante los últimos 10 años? ¿Durante los últimos cinco años? ¿Cuántas dependencias se vieron afectadas?

[3] Se utiliza un resumen criptográfico total para verificar la integridad y precisión de los datos. Si existen cambios o puntos faltantes, el nuevo resumen criptográfico total no se conciliará con el original.

[4] Esos procedimientos pueden utilizarse para entender el flujo de información dentro del proveedor de servicios e identificar dónde pueden explotarse las vulnerabilidades. Más aún, identifica en forma eficaz las autoridades dentro del proveedor de servicios, facilitando la identificación de responsabilidades en caso accidental de revelación de información o uso no autorizado. Los controles de permiso (es decir, leer, escribir, ejecutar, borrar) se diseñan en base a la estructura de responsabilidades y autoridad. Esto proporciona un control más estricto en términos de modificación y fabricación de datos.

- Disponibilidad de contramedidas: ¿Está disponible alguna solución de mejores prácticas en la industria? Si no, ¿existe otra manera de contrarrestar esta amenaza?
- Preparación de los proveedores de servicio: ¿Están observándose las políticas, contratos de nivel de servicio y procedimientos en caso de escalada? ¿Cuánto tiempo les tomará a los proveedores de servicios resolver esta amenaza?
- Susceptibilidad de los suscriptores: ¿Están conscientes los suscriptores de tal amenaza? ¿Cuál es la probabilidad de que los suscriptores revelen su información en forma voluntaria si se enfrentan a dicha amenaza? ¿Puede un suscriptor distinguir fácilmente un acto malicioso de un acto genuino cuando se enfrenta a este tipo de amenaza?

2) **Análisis de riesgos.** Los riesgos pueden analizarse por el nivel del impacto de sus consecuencias y por la probabilidad de que ocurran. Este tipo de análisis proporcionará un conjunto de prioridades ordenadas grosso modo por costos esperados. Un ejemplo de este principio se presenta en la Tabla 2.

3) **Monitoreo de riesgos.** Una vez que se ha reducido el riesgo identificado, es importante que un equipo designado monitoree su desempeño y lo evalúe contra experiencias previas. El equipo deberá elaborar una lista de verificación de los problemas que se encuentren antes de solucionar la amenaza. Después, el mismo equipo deberá monitorear la estabilidad y eficacia de las medidas adoptadas y analizar cuidadosamente el sistema en busca de nuevas amenazas potenciales. Estas observaciones deben registrarse junto con la lista de verificación original y reportarse a los propietarios de los negocios.
   - Auditoría del sistema: Estructura de control fundamental que examina, verifica y corrige fallas y lagunas en ciertas funciones del sistema. Se exhorta a los proveedores de servicios a que lleven a cabo auditorías del sistema en forma regular, para asegurarse de que se resuelvan las vulnerabilidades del sistema y que no esté pasándose por alto ninguna actividad maliciosa. Lo anterior resulta especialmente esencial cuando se prueba la funcionalidad de sistemas desarrollados recientemente.
   - Análisis de brecha: Extensión de la lista de verificación que se menciona anteriormente. Es una herramienta eficaz para diferenciar las brechas de desempeño en términos de la funcionalidad del sistema. Aquí se presenta en una matriz que compara el desempeño actual y el esperado y la clasificación del componente analizado.

Conclusión

Ahora podemos unificar estas discusiones acerca de los flujos de información, amenazas y riesgos de los SFM, así como los principios y procedimientos utilizados para resolver las vulnerabilidades de los SFM.

Cualquier estrategia de solución debe empezar por localizar la vulnerabilidad dentro de la red de los flujos de datos de SFM. Por lo tanto, resulta fundamental que los entes reguladores cuenten con un entendimiento básico de la arquitectura de los sistemas de SFM, en especial la forma en que la información se mueve de un elemento de la red a otro. Con dicho entendimiento, los entes reguladores pueden aislar las vulnerabilidades que se derivan de la manera en que un elemento de la red maneja la información. Al identificar dichas vulnerabilidades del manejo de información, los entes reguladores pueden entonces evaluar cuál de las amenazas identificadas en la Tabla 1 tiene mayor probabilidad de poner en riesgo la red de SFM. La presencia de dichas amenazas infringe los principios de la protección de datos que se resumen en el apartado titulado “Identificación de riesgos tecnológicos de los SFM”. Como resultado, tanto la información financiera como la no financiera están sujetas a riesgos tecnológicos específicos.
El análisis de riesgos puede determinar cuál de los conceptos indicados en el registro de riesgos tiene la probabilidad de ocurrir y tener un mayor impacto en los consumidores.

Cuando se ingresan medidas de probabilidad e impacto, el registro de riesgos los ordena por su clasificación (de mayor a menor). Con una lista de riesgos por orden de prioridad, los entes reguladores pueden identificar, nivel por nivel, los tipos de controles de seguridad que se requieren para reducir dichos riesgos. Estos controles de seguridad se convertirán en la referencia para crear e implementar políticas públicas que aborden riesgos tecnológicos en el entorno de los SFM. La tabla a continuación presenta una muestra de cómo puede realizarse dicho análisis.

Tabla 3: Vulnerabilidades y controles de seguridad recomendados

Lugar del riesgo (elemento de la red)	Amenaza	Principio que se infringe	Riesgo probable	Controles de seguridad recomendados
Aplicación de la red móvil	• Revelación • Interceptación	Confidencialidad	Se ha leído información crítica enviada vía SMS	• Los números de cuenta del cliente se cifran cuando se transmiten • Los NIPs del cliente se cifran cuando se muestran y transmiten
Teléfono del usuario final	• Modificación	• Integridad • Autenticación	Infección causada por software malicioso móvil	• Las políticas de información por el lado de la red pueden descargarse en los teléfonos • Uso de antivirus específico para teléfonos inteligentes
Centro SMS, aplicación de SFM, red bancaria	• Interrupción	• Disponibilidad • Irrefutabilidad	Ataques de denegación de servicio	• Implementar un sistema que restrinja el tiempo de respuesta del paquete • Requerir que los SFM establezcan un entorno de red de alta seguridad, al adaptar las normas de mejores prácticas de seguridad como la ISO9001
Teléfono del usuario final	• Fabricación	• Autenticación • Irrefutabilidad	Ataques de suplantación de identidad *(phishing)*	• Solicitar una campaña activa de concienciación de los clientes, para instruir a los consumidores acerca de mensajes maliciosos • Exhortar a los consumidores/ víctimas a que reporten el número de los atacantes maliciosos a los proveedores de servicios de telecomunicaciones, para que puedan enviarse mensajes de advertencia y bloquear el número celular en forma permanente

Referencias

AUJAS. 2011. Mitigating Security Risks in USSD-based Mobile Payment Applications. http://www.thectoforum.com/content/mitigating-security-risks-ussd-based-mobile-payment-applications. [Accessed 26 July 2011].

BEVIS, J. 2007. Disaster Recovery – Alternate Site Geographical Distance. http://infosecalways.com/2007/12/19/disaster-recovery-%E2%80%93-alternate-site-geographical-distance./ [Accessed 24 July 2011].

BOCAN, V. & CREDU, V. 2006. Mitigating Denial of Service Threats in GSM Networks. In: GSM, C.A.P.I. (ed.).

DEPARTMENT OF PREMIER AND CABINE. 2009. Tasmanian Government Information Security Guideline. http://www.egovernment.tas.gov.au/__data/assets/pdf_file/0004/89185/Information_Security_Guidelines.pdf [Accessed 23 July 2011].

DHILLON, G. 2007. Principles of Information Systems Security: Text and Cases. John Wiley & Sons Inc.

GOSTEV, A. 2006. Mobile Malware Evolution: An Overview, Part 1. SECURELIST [Online].

HICKS, S. 2006. Mobile and Malicious: Security for mobile devices getting critical: best practices and technologies. Enterprise Networks & Servers [Online].

JUUL, N.C. 2002. Security Issues in Mobile Commerce using WAP. http://medusa.sdsu.edu/network/security/wap-bled.pdf.

LEE, P. 2002. Cross-site scripting http://www.ibm.com/developerworks/tivoli/library/s-csscript/ [Accessed 26 July 2011].

PELTIER, T. 2001.Information Security Risk Analysis. In: ASSET IDENTIFICATION: NETWORK AND SOFTWARE, P. A. O. A. (ed.). CRC Press LLC.

SAHIBUDIN, S., SHARIFI, M. & AYAT, M. 2008. Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Service providers. IEEE Computer Society, 749-754.

ZROBOK, D. 2001. The Security Issues with WAP. http://hygelac.cas.mcmaster.ca/courses/SE-4C03-01/papers/Zrobok-WAP.html [Accessed 26 July 2011].

Acerca de las Notas de Orientación del Grupo de Trabajo de Servicios Financieros Móviles de AFI

Las notas de orientación del Grupo de Trabajo de Servicios Financieros Móviles de AFI se basan en la experiencia de sus miembros e intentan proporcionar una guía para la definición de normas, enfoques y prácticas comunes para la regulación y supervisión de los SFM dentro de las instituciones miembros de AFI. Las notas no son resúmenes de mejores prácticas ni proponen nuevos principios o modificaciones a los principios fundamentales existentes. En cambio, resaltan los problemas de políticas y regulaciones clave de los SFM e identifican los retos a solucionar. Las definiciones que aquí se presentan tienen la intención de complementar, más que de reemplazar definiciones similares de SFM elaboradas por los Organismos Internacionales que Establecen Normas (SSBs, por sus siglas en inglés).

Acerca de AFI

La Alianza para la Inclusión Financiera (AFI) es una red mundial de bancos centrales y otros entes formuladores de políticas financieras de países en desarrollo. AFI proporciona a sus miembros las herramientas y los recursos para compartir, desarrollar e implementar sus conocimientos acerca de políticas de inclusión financiera. AFI conecta a los formuladores de políticas públicas a través de canales en línea y directos, apoyados por subvenciones y vínculos con organismos estratégicos asociados, con el fin de que dichos formuladores puedan compartir sus perspectivas e implementar las políticas de inclusión financiera más adecuadas para las circunstancias individuales de sus países.

Conozca más: www.afi-global.org

Alianza para la Inclusión Financiera

AFI, 399 Interchange Building, 24th floor, Sukhumvit Road, Klongtoey – Nua, Wattana, Bangkok 10110, Tailandia
t +66 (0)2 401 9370 **f** +66 (0)2 402 1122 **e** info@afi-global.org www.afi-global.org
www.facebook.com/AFI.History @NewsAFI

AFI es financiada por la Fundación Bill y Melinda Gates y administrada por GIZ (Agencia de Cooperación Internacional Alemana)