Mobile Financial Services Working Group (MFSWG)

Alliance for Financial Inclusion
Bringing smart policies to life

Services Financiers Mobiles
Risques technologiques

La présente Note Directrice a été élaborée par le Groupe de Travail sur les Services Financiers Mobiles de l'AFI (MFSWG) afin d'identifier d'une part les différents types de risques technologiques relatifs aux services financiers mobiles et d'autre part les stratégies de gestion de ces risques.

Note directrice N°2
Juillet 2013

Table des matières

Reconnaissant le potentiel des Services Financiers Mobiles (MFS), le Groupe de Travail sur les Services Financiers Mobiles (MFSWG) a été créé pour servir de plate-forme au sein du réseau de l'AFI en permettant aux décideurs de discuter des questions réglementaires liées aux MFS. Le Groupe de Travail encourage la large utilisation des MFS en tant que solution clé pour une plus grande inclusion financière dans les pays en développement et émergents. Le Groupe vise à stimuler la discussion et l'apprentissage parmi les décideurs et à promouvoir une plus grande coordination entre les nombreux différents acteurs en matière de MFS, tels que les régulateurs financiers et des télécommunications et les prestataires bancaires et non bancaires.

Contexte

Les Services Financiers Mobiles (MFS) offrent la possibilité d'une plus grande efficacité et de commodité dans les applications de paiement et pourraient également servir de base à des initiatives d'inclusion financière. Cependant, pour que les MFS tiennent leurs promesses, les fournisseurs de services et les régulateurs doivent considérer sérieusement la sécurité des plateformes au sein de ce nouveau marché.

Étant donné que les modèles commerciaux, les besoins de marché, et l'abstention réglementaire varient d'un pays à l'autre, cette note ne donne pas un ensemble unique de politiques appropriées à tous les contextes. Par contre, il est destiné à aider l'orientation de l'élaboration des politiques en identifiant les types de risques technologiques endémiques aux services financiers mobiles et les stratégies pour les gérer. Cette note définit donc les flux d'informations dans les transactions liées à des MFS, identifie les types de risques technologiques associés connexes, et articule les cadres de gestion et de surveillance de ces risques. Le but de cette note est d'aider les régulateurs à commencer à penser à des risques technologiques associés aux MFS d'une manière souple qui sera utile pour la prise de décisions futures.

Une note sur la langue : tout au long de cette note, le terme « ***menaces*** » est utilisé pour décrire les catégories de dysfonctionnement concernant l'offre des MFS et « ***risques*** » se réfère à l'application de ces menaces aux processus réels impliqués dans la prestation des MFS. En ce sens, les risques sont les cas de menaces observables dans le monde réel des transactions.

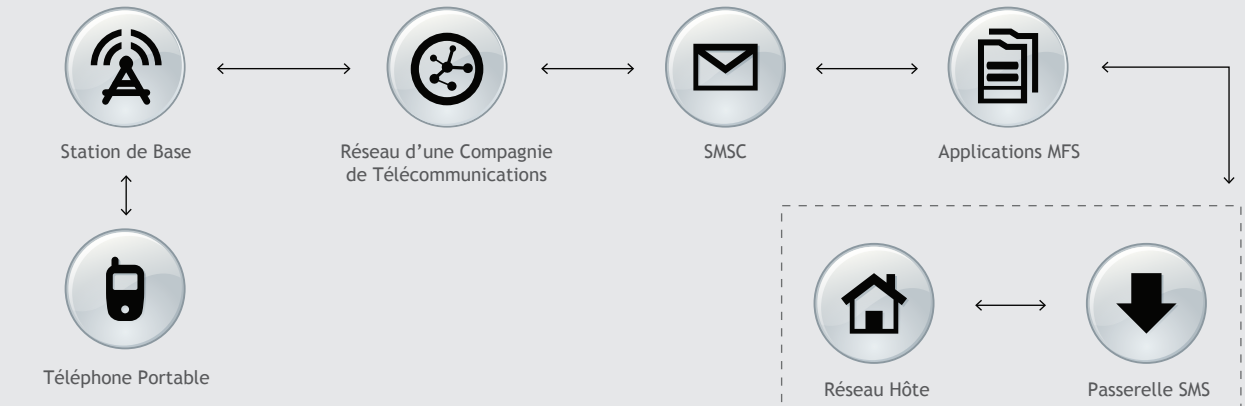
Flux d'information en matière de MFS

Les régulateurs doivent se familiariser avec la façon dont l'information circule au sein du réseau des MFS afin d'analyser les risques techniques qui évoluent dans cet environnement. Si vous comprenez comment chacune des composantes dans le réseau gère les informations, vous pouvez donc identifier les types de contrôles nécessaires pour garantir la sécurité de ces informations. La figure 1 est une représentation schématique de ces flux d'information pour un service bancaire fondé sur les MFS offert en partenariat avec un Opérateur de Réseau Mobile (ORM).

Infrastructure MFS (utilisant la technologie STK)

Les utilisateurs des MFS lancent des processus en utilisant leurs téléphones portables. Les informations fournies par chaque utilisateur sont alors envoyées à la station de base de l'ORM.[1] Dans un réseau GSM, la station de base reçoit une demande du canal de l'appareil de communication mobile et la transmet à l'ORM de l'utilisateur. Grâce aux transactions SMS, les paquets de données contenant des informations de transaction sont traités dans un centre de service de messages courts (SMSC) et acheminé vers le serveur d'application des MFS. À son tour, le serveur d'application des MFS transmet les détails de transaction à une passerelle — l'interface entre le Réseau de l'opérateur mobile et le réseau de la banque. Le paquet de données est ensuite soumis à un contrôle de sécurité, et en attendant l'autorisation, acheminé vers le réseau interne de la banque pour l'autorisation et le traitement ultérieur. Le réseau de la banque stocke des informations financières et non financières de l'utilisateur et autorise la transaction demandée par l'utilisateur. Puisque ce processus fonctionne en sens inverse, c'est à ce moment que l'utilisateur est informé de la transaction complétée.

Figure 1 : infrastructure de Services Financiers Mobiles (utilisant la technologie STK)



Infrastructure MFS (Utilisant la technologie STK)

[1] Tous les messages envoyés par le téléphone portable possèdent un code d'identification qui est utilisé par la station de base pour déterminer si le réseau utilisé par l'expéditeur lui appartient. Si c'est le cas, le message est transmis au réseau de l'opérateur de télécommunications. Sinon, le message sera supprimé. Le téléphone portable continuera alors à chercher une station de base qui répondra à sa demande jusqu'à ce qu'une poignée de main complète soit établie.

Classification des menaces technologiques

Il est important de comprendre les flux d'informations relatifs aux opérations des MFS, car un certain nombre de risques technologiques sont présents à chaque étape de ces flux. En effet, il est essentiel de classifier les risques technologiques selon les catégories de menace les plus importantes. Dhillon (2007) identifie six catégories générales de menaces liées aux systèmes d'information :

Modification — lorsque l'information dans le système est accédée sans autorisation et troquée sans autorisation.

Destruction — lorsque le matériel, les logiciels, les données ou les canaux de communication sont détruits ou perdus.

Divulgation — lorsque les données sont mises à disposition sans le consentement du propriétaire.

Interception — lorsqu'une personne ou un logiciel non autorisé accède aux ressources d'informations, permettant ainsi à des programmes et autres informations confidentielles d'être copiés sans autorisation.

Interruption — lorsque les services ou les ressources ne sont pas disponibles pour l'utilisation, que ce soit accidentellement ou intentionnellement.

Falsification — lorsque les fausses transactions sont introduites dans un document ou ajoutées à une base de données par un utilisateur non autorisé.

Comme résumé dans le tableau 1, ces menaces décrivent les risques associés et s'appliquent au diagramme montrant le processus de flux d'information relatifs aux services financiers mobiles.

La 2e figure présente une vue non exhaustive des points au niveau desquels les menaces peuvent être introduites dans les flux d'information des MFS.

Tableau 1 : Classification des menaces technologiques associées aux MFS

Menaces	Données	Logiciel	Matériel	Canaux de communication
Modification	Se produit pendant le stockage, le transport et le changement du matériel physique	Se produit lorsque le logiciel est modifié de façon à exécuter des fonctions ou des calculs supplémentaires	–	Se produit lorsque les paquets sont acheminés vers une autre destination
Destruction	Est causé par une défaillance du matériel et / ou du logiciel	Destruction due à une intention malveillante, c'est à dire un logiciel malveillant (malware)	Est causé par les calamités naturelles telles que les inondations, les incendies, ou les attaques terroristes	Est causé par les coupures des fibres optiques ou des lignes louées en raison d'événements imprévus comme par exemple les inondations, le vol, ou la construction des routes
Divulgation	Se produit quand il y a un accès non autorisé aux données / informations d'une autre personne	–	–	–
Interception	Se produit lorsque des renseignements confidentiels sont dupliqués par des utilisateurs non autorisés	Se produit lorsque des logiciels sont illégalement copiés à partir d'une ressource informatique	Se produit lorsque des utilisateurs non autorisés accèdent au matériel physique	Se produit lorsqu'un tiers a pu sous-écouter (écouter) et intercepter une information à l'insu des utilisateurs légitimes
Interruption	–	Se produit quand des logiciels et/ou fonctionnalités spécifiques sont effacés du système Cela est peut-être le résultat de la détérioration du système d'exploitation	Est causé par un matériel endommagé	Est causé par les attaques malveillantes, telles que l'inondation et les attaques types de déni-de-service Est peut-être le résultat des catastrophes naturelles, panne d'électricité, problèmes de stations de base, ou problèmes de réseau
Falsification	Est causé par les attaques d'hameçonnage	–	–	–

Référence : Dhillon, G. (2007) *Principles of Information Systems Security: Text and Cases.*

Identification des risques technologiques associés aux MFS

Le cadre de classification fourni par le langage des menaces peut nous aider à donner un sens à la profusion des risques technologiques qui affectent les MFS. Ces risques sont spécifiques et variés, mais une fois placés sous l'essence de menaces, ils peuvent nous aider à organiser, éviter et, éventuellement, y remédier. Cette section met en lumière les risques spécifiques et les organise en fonction de la plus grande catégorie des menaces auxquelles ils appartiennent.

Menace : Modification

Infection par des logiciels malveillants mobiles (risque)

Les attaques à partir des logiciels malveillants sont fréquentes dans l'environnement des PC et on s'attend à ce qu'elles se répandent soudainement et rapidement à des appareils mobiles. Les attaques à partir des logiciels malveillants visant les téléphones mobiles peuvent se produire comme suit[2] :

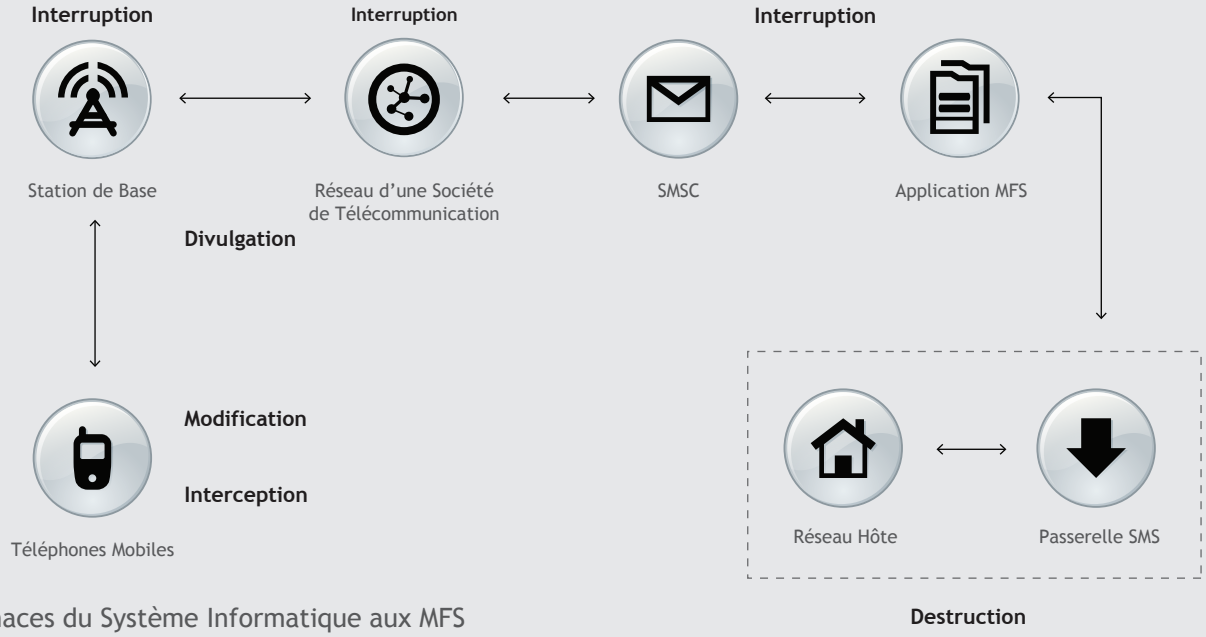
- les virus malveillants / chevaux de Troie / les virus peuvent se propager via Bluetooth et MMS ;
- les logiciels malveillants peuvent manipuler un utilisateur par l'envoi des SMS ;
- les logiciels malveillants peuvent infecter les fichiers ;
- Ceux qui attaquent le système par propagation de logicels malveillants peuvent accéder à distance aux téléphones mobiles ;
- les logiciels malveillants, une fois téléchargés, peuvent changer les icônes et les applications de système ;
- les logiciels malveillants peuvent installer des fonctions et des applications non opérationnelles ;
- les logiciels malveillants sont un canal utile pouvant être utilisé pour installer d'autres programmes malveillants ;
- les logiciels malveillants peuvent voler toute donnée ou information saisie par l'utilisateur et bloquer l'utilisation des cartes mémoires.

Menace : Divulgation

Lisibilité des informations financières cruciales des clients par SMS (risque)

La lisibilité est une préoccupation majeure lors de l'utilisation des SMS pour accéder aux comptes et recevoir des notifications sur les activités antérieures. Les SMS sont transmis et reçus en texte clair et ce protocole n'utilise pas des techniques de cryptage. En cas de vol d'un téléphone mobile et l'utilisation des logiciels malveillants, les utilisateurs non autorisés peuvent obtenir un accès complet au compte d'un client.

Figure 2 : Menaces du système informatique aux MFS



Menaces du Système Informatique aux MFS

[2] Gostev, A., 2006.

Menace : Divulgation

Exposition des données importantes en raison d'un cryptage bout à bout non sécurisé (risque)

Le Protocole d'application sans fil (WAP) est une norme d'application qui permet aux téléphones mobiles d'accéder à Internet. Les téléphones mobiles équipés du WAP utilisent des navigateurs similaires à ceux utilisés par les ordinateurs, même s'ils sont modifiés pour tenir compte des restrictions de téléphones mobiles. Le WAP utilise la même approche à plusieurs niveaux que celle des couches TCP-IP. Un site web normal informatique permet aux utilisateurs d'accéder à Internet en utilisant le protocole de couche d'application HTML. De même, les consommateurs ayant des téléphones équipés du WAP peuvent accéder au même site en utilisant leurs téléphones mobiles au moyen du Protocole WML (Wireless Markup Language), qui est une couche d'application du WAP. La seule différence entre les deux étant la taille et la résolution de l'écran (car le site est transformé pour répondre aux restrictions du téléphone portable). Les transmissions non chiffrées sont donc vulnérables à l'exposition à des tiers non autorisés.

Menace : Interruption

Indisponibilité du canal de communication en raison des attaques de type déni-de-service (risque)

Les attaques de type déni-de-service (DOS) font en sorte qu'une ressource informatique devient indisponible en inondant ou en consommant les ressources du composant. Le plus souvent, les attaques DOS visent les serveurs et les bases de données, qui peuvent également affecter les réseaux mobiles, car l'environnement câblé et sans fil utilise la même infrastructure.

Menace : Interception

Attaque sur les éléments dynamiques dans USSD (risque)

Le protocole de communication USSD permet une transmission des données plus rapide par rapport aux SMS. Contrairement aux SMS, le protocole USSD utilise une connexion directe entre l'expéditeur et le destinataire. Il s'agit d'un canal de communication orienté vers une session dans laquelle l'application USSD est utilisée comme interface entre l'opérateur de télécommunication et le compte bancaire du client. De même, le protocole USSD peut être géré à l'aide des applications Web et il est donc vulnérable aux attaques sur les éléments dynamiques. Lors de ces attaques, un utilisateur malveillant exploite la vulnérabilité de l'application Web installée dans le téléphone mobile de l'utilisateur pour manipuler les transactions (en injectant un script Java ou SQL pour voler des informations importantes de l'utilisateur). Il peut également effectuer des actions malveillantes dans la base des données, s'emparer de la session active d'un autre utilisateur, et connecter les utilisateurs aux serveurs malveillants.

Cette liste de risques n'est pas exhaustive, mais elle illustre les types de risques que tout prestataire de services doit gérer. Ayant ces risques à l'esprit, nous nous penchons maintenant sur les principes de gestion et de contrôle des risques dont les régulateurs doivent être conscients.

Tableau 2 : Modèle d'impact des risques

PROBABILITÉ	IMPACT				
	Catastrophique	Haut	Modéré	Faible	Insignifiant
Presque certain	E	E	E	H	M
Probable	E	E	H	H	M
Possible	E	E	H	M	F
Peu probable	E	H	M	F	F
Rare	H	H	M	F	F

NIVEAU DE RISQUE : E = Extrême H = Haut M = Modéré F = Faible

Risques technologiques associés aux MFS : gestion et suivi

PRINCIPES

Il y a cinq grands principes qui orientent la gestion des risques technologiques associés aux MFS : Confidentialité, Intégrité, Disponibilité, Authentification et Non-répudiation. Chacun de ces principes est analysé ci-dessous.

Confidentialité : il s'agit de protéger les données des utilisateurs contre tout accès non autorisé ou vol. Il est important de faire la distinction entre les données financières et non financières parce que les différents principes de confidentialité s'appliquent à toutes ces données. En général, les données financières nécessitent les normes d'encryptage les plus forts dans l'affichage, le stockage et la transmission. Les Numéros d'identification personnels doivent être stockés sous forme cryptée et ne doivent pas être disponibles au personnel du fournisseur de service. De fortes normes de cryptographie doivent être appliquées aux données transmises sur des réseaux publics, tels que les réseaux Internet et cellulaires. Les données non financières peuvent être gardées confidentielles avec des étapes un peu moins strictes, telles que la création des pare-feu, la mise en œuvre des systèmes de prévention et de détection des intrusions, et l'utilisation des mesures de contrôles d'accès.

Intégrité : il s'agit de l'exhaustivité, l'exactitude et la fiabilité des données présentées. C'est dans le but de valider l'intégrité des données, vérifier le processus qui identifie les champs manquants, effectuer des contrôles de séquence, et vérifier le total de hachage[3] et la longueur variable. L'intégrité des données est plus importante lors de la transmission car la manipulation et l'interception des données sont plus susceptibles de se produire à ce stade.

Disponibilité : les données et les services devraient être accessibles à tout moment où les utilisateurs légitimes souhaitent utiliser les MFS. Il y a un certain nombre de scénarios qui peuvent menacer les données et la disponibilité des services. Les risques techniques liés à la disponibilité des services comprennent les catastrophes environnementales (telles que les coupures de l'électricité, les attaques terroristes et les actes naturelles) et les actions malveillantes telles que les attaques de types déni-de-services.

Authentification : il s'agit d'établir l'identité de l'utilisateur et du prestataire de services.

- Les **utilisateurs** doivent avoir la certitude que l'hôte demandant la connexion est autorisé et qu'il n'y a pas de tiers impliqués dans la connexion entre le terminal et le serveur de l'hôte. Cela inclut également le contrôle de l'accès, le contrôle de l'autorisation et l'authentification du mot de passe.
- Les **prestataires de services** doivent être convaincus que la personne qui accède aux données est bien celle qu'elle prétend être. Les journaux d'audit évaluent la validité et la cohérence des données circulant dans le réseau et sont des outils importants permettant de vérifier si les commandes ont été exécutées par des utilisateurs légitimes. En tant que tel, les régulateurs doivent être en mesure d'examiner la façon dont les fournisseurs de services surveillent les journaux d'audit. De même, les procédures de gestion et opérationnelles devraient être établies pour contrôler l'accès à l'information des clients et maîtriser les vulnérabilités du système.[4]

Non-répudiation : il s'agit de l'autoprotection du fournisseur de services contre les comportements abusifs possibles de la part des consommateurs et des employés, en assurant le caractère définitif et la sécurité des transactions. Il est utile de s'assurer que les personnes se conviennent sur les termes et modalités de service avant toute action et sur l'utilisation des signatures numériques car cela les empêche de nier leurs actions. Les principaux certificats publics permettent également aux fournisseurs de services de retracer l'origine de la transaction au cas où il n'y aurait pas d'échange direct d'informations entre les entités.

Ces principes offrent un cadre pour comprendre les vulnérabilités des MFS qui est complémentaire à la discussion sur les menaces et les risques. L'interprétation de menaces en tant que violations des principes spécifiques de gestion de base peut aider à déterminer la réponse réglementaire nécessaire. Le processus de gestion des risques permet de continuer à formuler et calibrer cette réponse.

PROCESSUS

La gestion des risques se déroule par étape : (1) l'évaluation des risques, (2) l'analyse de ces risques en fonction de l'impact attendu et la probabilité, et (3) le suivi de ces risques en fonction des attentes de l'impact possible et de la probabilité.

---

[3] Un total de hachage est utilisé pour vérifier l'exhaustivité et l'exactitude des données. S'il y a des changements ou des éléments manquants, le nouveau total de hachage ne se réconciliera pas avec l'original.

[4] Ces procédures peuvent être utilisées pour comprendre les flux d'informations claires au sein du fournisseur des services et déterminer où les vulnérabilités peuvent être exploitées. En outre, elles identifient de manière efficace les autorités au sein du fournisseur de services, ce qui rend plus facile de déterminer les responsabilités en cas de divulgation accidentelle ou l'utilisation non autorisée des renseignements. Les contrôles d'autorisation (c'est-à-dire, lire, écrire, exécuter, supprimer) sont conçus sur la base de la structure de responsabilité et d'autorité. Cela donne un contrôle plus strict en termes de modification et de falsification des données.

1) **Évaluation des risques.** Les critères d'évaluation permettent d'évaluer profondément des menaces potentielles face au système. Les critères suivants sont proposés pour les MFS :

   - Faisabilité d'une menace : cette menace s'est-elle déjà produite ? Quelles composantes ont été touchées ? Logiciel ? Canal ? Combien de temps a-t-on mis avant d'identifier cette menace ?
   - Incidents enregistrés : combien de fois cette menace s'est-elle produite au cours des 10 dernières années ? Au cours des cinq dernières années ? Combien d'agences ont été touchées ?
   - Disponibilité des contre-mesures : y a-t-il une solution fondée sur les meilleures pratiques du secteur disponible ? Sinon, y a-t-il un autre moyen pour faire face à cette menace ?
   - Préparation des fournisseurs de services : les politiques, les accords de niveau de service et les mesures subséquentes graduelles sont-ils suivis ? Combien de temps faut-il pour que les fournisseurs de services réagissent à cette menace ?
   - Susceptibilité des abonnés : les abonnés sont-ils conscients d'une telle menace ? Quelle est la probabilité pour les abonnés de divulguer volontairement leurs renseignements face à une telle menace ? Un abonné peut-il facilement distinguer un acte malveillant d'un acte véritable face à ce type de menace ?

2) **Analyse des risques.** Les risques peuvent être analysés par l'impact de leurs conséquences et par leurs probabilités d'occurrence. Ce type d'analyse fournira un ensemble de priorités à peu près ordonné par les coûts attendus. Une illustration de ce principe est présentée dans le tableau 2.

3) **Suivi des risques.** Une fois que le risque identifié ait été atténué, il est important que l'équipe désignée surveille sa performance et l'évalue par rapport aux résultats précédents. L'équipe doit dresser une liste des problèmes rencontrés avant de traiter le risque. Après le traitement, la même équipe doit surveiller la stabilité et l'efficacité de l'action prise et analyser attentivement le système afin d'identifier de nouvelles menaces possibles. Ces observations doivent être enregistrées à côté de la liste de contrôle d'origine et signalées aux propriétaires de l'entreprise.

   - Audit du système : c'est une structure de contrôle fondamentale qui examine, vérifie et corrige les défauts et comble les lacunes de certaines fonctions du système. Les fournisseurs de services sont encouragés à effectuer régulièrement des audits de système afin de s'assurer que les vulnérabilités du système sont traitées et qu'aucune activité malveillante n'est négligée. Cela est particulièrement essentiel pour tester la fonctionnalité des systèmes nouvellement déployés.
   - Analyse des lacunes : c'est une extension de la liste de contrôle précédemment mentionnée, il s'agit d'un outil efficace pour différencier les écarts de performance en termes de fonctionnalité du système. Ici, il est présenté dans une matrice qui compare la performance actuelle et celle prévue et qui classifie la composante analysée.

Conclusion

Nous pouvons maintenant unifier ces discussions sur les flux d'informations des MFS, les menaces et les risques, ainsi que les principes et les procédures utilisées pour remédier aux vulnérabilités des MFS.

Toute stratégie de réponse doit partir de la localisation de la vulnérabilité au sein du réseau des flux des données MFS. Il est donc essentiel que les régulateurs aient une connaissance de base de l'architecture des systèmes MFS, en particulier, la façon dont l'information passe d'un élément du réseau à l'autre. Grâce à cette compréhension, les régulateurs peuvent ensuite isoler les vulnérabilités découlant de la façon dont un élément du réseau traite les informations. En identifiant ces vulnérabilités relatives au traitement d'informations, les régulateurs peuvent alors évaluer laquelle de ces menaces identifiées dans le tableau 1 est la plus susceptible de compromettre le réseau MFS. La présence d'une telle menace viole les principes de protection des données énoncées à la section d'identification des risques technologiques relatifs aux MFS. En conséquence, les informations financières et non financières sont soumises à des risques technologiques spécifiques. L'analyse des risques permet de déterminer lequel des éléments indiqués dans le registre des risques a plus de probabilité d'apparaître et lequel aura le plus d'impact sur les consommateurs.

Une fois rempli par des mesures de probabilité et d'impact, le registre des risques classifie les risques par leurs classements (en ordre décroissant). Avec une liste hiérarchisée des risques, les régulateurs peuvent, étage par étage, identifier les types de contrôles de sécurité nécessaires pour atténuer ces risques. Ces contrôles de sécurité deviendront la base de référence pour la conception et la mise en œuvre des politiques qui répondent aux risques technologiques dans l'environnement des MFS. Le tableau 3 ci-dessous montre un exemple de la façon dont cette analyse peut être effectuée.

Tableau 3 : Vulnérabilités et contrôles de sécurité recommandés

Site du risque (Élément du réseau)	Menaces	Principe violé	Risque probable	Contrôles de sécurité recommandés
Application du réseau mobile	• Divulgation • Interception	Confidentialité	Informations critiques envoyées par SMS sont lues	• Les numéros de compte des clients sont cryptés lors d'envoi • Les NIP des clients sont cryptés lors d'affichage et d'envoi
Téléphone mobile de l'utilisateur	• Modification	• Intégrité • Authentification	Infection causée par les virus malveillants mobiles	• Les politiques de réseau relatives aux informations téléchargeables sur les téléphones mobiles • L'utilisation d'anti-virus spécifiquement conçus pour les smart phones (téléphones sophistiqués)
Centre SMS, Application MFS, Réseau de banque	• Interruption	• Disponibilité • Non-répudiation	Attaque de type déni de service	• Mettre en place un système qui limite le temps de réponse des paquets • Exiger que les MFS établissent un environnement de réseau hautement sécurisé en adaptant les normes de sécurité en matière de meilleures pratiques comme ISO9001
Utilisateur final du téléphone mobile	• Falsification	• Authentification • Non-répudiation	Attaques de hameçonnage	• Exiger une campagne active de sensibilisation des clients pour informer les consommateurs au sujet des messages malveillants • Encourager les consommateurs / victimes à signaler les numéros portables des attaquants malveillants aux fournisseurs de services de télécommunications afin que les messages d'alerte puissent être envoyés et que les numéros des téléphones mobiles soient bloqués de façon permanente

Bibliographie

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].

À propos des notes directrices du Groupe de Travail Sur les Services Financiers Mobiles de l'AFI

Les Notes Directrices du Groupe de Travail Sur les Services Financiers Mobiles de l'AFI se basent sur l'expérience des membres et tentent de donner des directives supplémentaires en ce qui concerne la définition des normes, des approches et des pratiques communes pour la réglementation et la supervision des MFS au sein des institutions membres de l'AFI. Les notes ne résument pas les meilleures pratiques et elles ne proposent pas non plus de nouveaux principes ni une révision des principes de base existants. Par contre, elles mettent en évidence les principales questions politiques et réglementaires relatives aux MFS et identifient les défis à relever. Enfin, les présentes définitions sont destinées à compléter plutôt qu'à remplacer les définitions similaires des MFS élaborées par les organismes internationaux de normalisation financière.

À propos de l'AFI

L'Alliance pour l'Inclusion Financière (AFI) est un réseau mondial de banques centrales et d'autres organismes financiers chargés de l'élaboration des politiques en matière d'inclusion financière des pays en développement. L'AFI fournit à ses membres des outils et des ressources permettant de partager, de développer et de mettre en oeuvre leurs connaissances des politiques d'inclusion financière. Soutenu par des subventions et des liens avec des partenaires stratégiques, le réseau de L'AFI permet aux décideurs politiques et régulateurs, à travers des canaux en ligne et face-à-face, de partager leurs connaissances et de développer des politiques d'inclusion financière à mettre en oeuvre qui soient appropriées aux circonstances respectives de leur pays individuels.

Pour en savoir plus : www.afi-global.org

Alliance pour l'Inclusion Financière

AFI, 399 Interchange Building, 24th floor, Sukhumvit Road, Klongtoey – Nua, Wattana, Bangkok 10110, Thaïlande
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

L'AFI est financée par la Bill & Melinda Gates Foundation et administrée par la GIZ (Coopération internationale allemande)