MANDATS VIRTUELS ET CYBERCRIME

Par F.B. Huyghe

En février de cette année MasterCard et GSM Association (GSMA) ont annoncé la création d'un système destiné à émettre et de recevoir des mandats internationaux par téléphone mobile. Dix-neuf opérateurs représentant environ 600 millions d'usagers dans cent pays s'associent à ce projet pour lequel un programme pilote est déjà lancé.

Le but est entre autres de permettre à des travailleurs migrants qui ne possèdent pas nécessairement de compte en banque d'envoyer facilement de l'argent aux leurs, partant du principe que le réseau mobile couvre bien mieux la planète que le réseau bancaire. Le potentiel de développement est impressionnant : à la fin 2004, GSMA regroupait plus de 660 opérateurs, desservant plus de 1,3 milliard de clients dans 210 pays.

Petites sommes, gros enjeux.

À titre de comparaison, en arrondissant les chiffres, 80% de la population mondiale est déjà couverte par les réseaux mobiles et il circule déjà 230 milliards de dollars de mandats par an dans le monde, en grande partie du fait des 200 millions de travailleurs migrants. Or, le système actuel des mandats internationaux de banque à banque ou de poste à poste n'est ni instantané, ni bon marché: il peut coûter jusqu'à 24% pour de petites sommes. Ce sont typiquement celles qu'un travailleur migrant aimerait envoyer à sa famille vite et au coup par coup.

De fait ce système d'argent numérique transférable existe déjà. Ainsi, aux Philippines, pays où plus de deux personnes sur cinq possèdent un téléphone mobile, des programmes comme Smart « padala » (« amène-moi mon argent » en filipino) et Globe Telecom's G-Cash permettent d'envoyer des messages valant virement. Ils sont payables en liquide dans les boutiques spécialisées.

Le principe du modèle philippin est le suivant : le téléphone de l'usager est relié à un compte en liquide préalablement alimenté. À partir de son mobile, le détenteur peut déposer de l'argent, en retirer, en transférer à un compte pré payé (pour recharger son crédit de service), ou à un autre usager. En somme, il peut coupler l'usage du téléphone comme medium de transaction et d'une carte de crédit classique.

Le système fonctionne de l'étranger : ainsi, un Philippin à Bahreïn peut envoyer des fonds au pays grâce à cette version digitale de la vieille lettre de crédit.
Le destinataire, une fois qu'il a reçu le message annonçant le virement, peut se le faire escompter dans une banque, ou une boutique, l'utiliser comme crédit sur son propre téléphone…
On notera au passage que la sécurité du système philippin est assurée par un simple code PIN (celui que nous tapons pour activer notre téléphone mobile) plus une carte SIM (les puces des téléphones, spécifiques à chaque propriétaire officiel). Tout repose donc sur la cryptologie.

En Corée du Sud, la fusion de fait entre carte de téléphone mobile (SIM) et carte bancaire passe au stade expérimental en Avril 2007. Ailleurs, il existe des systèmes comparables : Fundamp et MTN-Bank en Afrique du Sud ou Safaricom au Kenya ont développé des systèmes téléphoniques de micro payement.
Un projet international de l'ampleur de celui de GSMA pourrait d'après ses promoteurs doubler le nombre de destinataires des mandats internationaux qui passerait à 1,5 milliards par an. À l'horizon 2012, le marché du mandat international pourrait monter à mille milliards de dollars, ce qui représente à peu près quatre fois son niveau actuel Pour des pays comme l'Inde (déjà destinataire d'un mandat international sur 10 dans le monde et en pleine expansion) l'enjeu est énorme.

A priori, on pourrait se féliciter que l'argent circule mieux et sans frais disproportionnés, que les travailleurs expatriés puissent aider plus facilement leur famille, que les services bancaires deviennent plus accessibles aux pauvres (tout en les intégrant dans le système financier des riches), et que toutes ces initiatives contribuent à réduire la fracture numérique.

Par ailleurs, n'est-ce pas une tendance historique de l'argent que de se dématérialiser ? Si des milliards circulent tous les jours de Bourse à Bourse sous forme de bits informatiques et si les projets de type « porte monnaie numérique » se développent partout, il ne serait guère logique qu'un mandat continue à ressembler à un papier mal imprimé, plein de cases mystérieuses, nécessitant force coups de tampons et que l'on attend avec la prochaine tournée du facteur.

Donc tout va bien… À moins que…

Une opportunité pour le crime organisé

À moins que la criminalité internationale n'exploite les failles de ce système.

Des milliards de dollars vont circuler de pays à pays, vite, souvent, par petites sommes qui n'attirent guère l'attention, de ou vers des zones où il n'existe pas forcément des administrations fiscales et policières tatillonnes et incorruptibles. La traçabilité des opérations, en cas d'enquête internationale dépendra des disques durs d'opérateurs, téléphoniques ou bancaires, dispersés, soumis à des législations ou à des normes légales et à des techniques de contrôle très différentes. La vérification des noms et des adresses des acteurs (voire celle de leur simple existence) sera complexe. Tout se passera entre correspondants virtuels identifiés par un numéro et dont personne ne verra la tête.
Certains appartiendront à des communautés exilées et vivront des conditions où ils pourront être facilement soumis aux pressions. Nous venons de voir récemment comment les commerçants sri lankais pouvaient être rackettés par les Tigres Tamouls en plein Paris et payer une sorte d'impôt révolutionnaire. D'autres communautés payent, elles, à leurs mafias nationales (si tant est que la distinction politique/criminel soit toujours très claire). Pense-t-on sérieusement qu'un Pakistanais ou Vietnamien travailleur pauvre à des milliers de kilomètres de chez lui a les moyens de résister à l'amicale pression de gens qui lui demanderont de leur rendre un petit service tous les mois ? S'imagine-t-on que tout le dispositif technique chez les fournisseurs d'accès, les opérateurs, mémoires commutateurs, concentrateurs (*hubs*), routeurs pourra être facilement visité par un cyber-gabelou ?

Ce système complexe représentera d'incroyables opportunités pour tous les trafics et blanchissements. En tant que réseau planétaire, instantané, à multiples entrées, facilement anonyme, il est intrinsèquement vulnérable.
S'ajoute un second facteur. Tout passera par des téléphones mobiles. Or un combiné GSM est par nature un objet nomade, presque intime puisqu'on le porte toujours avec soi. Il est aussi un terminal relié à des flux numériques de voix, de textes, d'images, de données et maintenant d'argent circulant sous forme numérique, via une multitude de relais et vecteurs. Il conjugue toutes les faiblesses d'un ordinateur en termes de sécurité plus d'autres qui sont liées à son statut d'objet hybride.

Les criminels et à fortiori les cybercriminels recherchent les points faibles. Là où ils rencontrent l'équivalent d'une porte blindée, ils passent pas la fenêtre.
Sur les ordinateurs traditionnels, leurs attaques se sont déjà largement diversifiées ; ils pratiquent l'intrusion, l'espionnage, le vol d'identité, le « hammeçonnage » (inciter une victime à donner des informations confidentielles à l'aide, par exemple, d'un faux site), le déni de

service (fait de bloquer le fonctionnement d'un site) ; ils créent des virus et des logiciels malveillants… Ils prennent le contrôle de réseaux entiers de PC pour les faire participer à leurs offensives : on parle alors de machines zombies pour désigner ces ordinateurs qui échappent à leur propriétaire légitime et, à son insu, participent à une offensive de déni de service, de propagation de spam ou autre, décidée en fait par un manipulateur malveillant.

Et comme il existe des millions d'ordinateurs fonctionnant pour la plupart sous Windows, les pirates ont théoriquement des millions de cibles possibles dès qu'ils découvrent une faille de sécurité. En retour, les lignes de défense s'organisent. Lorsque Microsoft produit une nouvelle version de son système, Windows, Vista, la société de Bill Gates qui a investi des millions de dollars dans la sécurité sait très bien que les millions d'utilisateurs futurs sont très sensibles à cette question, que l'information sur une seule faille circulerait dans le monde entier en quelques heures, et que la riposte devrait être instantanée. Bref la lutte entre attaquants et défenseurs se déroule à grande échelle et à grand bruit. Nous connaissons à peu près les règles de cette guerre-là même si telle ou telle bataille peu réserver des surprises.

Mais il est un autre terrain que les pirates ont déjà commencé à investir : celui de la téléphonie. Les spécialistes de la sécurité sont unanimes à prédire le développement de la criminalité dans ce secteur pour des raisons assez évidentes. Pour prendre un exemple récent : des spécialistes de la sécurité comme Jimmy Shah de McAfee estiment dans le rapport annuel de cette institution que ce nombre d'attaques sur les téléphones mobiles aura doublé en 2007.

Téléphones mobiles et criminalité sans frontière

Le premier facteur est purement quantitatif : il s'agit d'un secteur prometteur en termes de développement.

Quelques indices :

- Il y aura bientôt trois milliard de détenteurs de téléphones mobiles dans le monde (environ trois fois plus que de comptes bancaires). Le mobile bas de gamme est accessible sinon au pauvre, du moins à une grande fraction de la population mondiale qui n'a pas nécessairement un logement fixe avec une ligne filaire et une connexion Internet. Ou qui, simplement, trouve plus pratique d'utiliser un mobile. Depuis quelques mois, en France, le nombre de GSM a dépassé celui des lignes filaires et il est très supérieur dans de nombreux pays du Sud.
- Selon la société de recherche In-Stat, le marché des smartphones (téléphones mobiles sophistiqués cumulant les fonctions d'un assistant personnel et capable de naviguer sur Internet) devait atteindre 250 milliards de dollars d'ici cinq ans.
- Lors de son dernier *Developper Forum*, la société Intel a confirmé son intention d'investir beaucoup d'efforts dans sa plate-forme Ultra Mobile 2007 destinée à des PC dits « ultra-portables », qui combineraient sous un format de poche les fonctions des meilleurs ordinateurs et la capacité de connecter aux réseaux cellulaires, au Wifi, au Wimax.
- La norme dite « 4 G » (téléphone mobile de quatrième génération) devrait apparaître l'an prochain. Elle permettrait entre autres des taux de transmission de données de 20 mégabits par seconde.

Donc, que l'on parle bas de gamme ou haut de gamme (et que l'on appelle les appareils sophistiqués des smartphones, des assistants personnels, des micro-ordinateurs…) toutes les courbes montent vers le ciel.

Corollaire : les téléphones portables sont des hybrides techniques de plus en plus compliquées. Il n'y a pas un système d'exploitation unique et universel à la Windows ou Unix mais un empilement de normes et de protocoles. Ce qui va de pair avec une autre tendance lourde. Les téléphones mobiles font de plus en plus de choses, ce qui signifie qu'ils reçoivent (et souvent téléchargent et mettent à jour) de plus en plus de programmes parvenant par des vecteurs de plus en plus variés (par les réseaux GSM, par Bluetooth, par Wifi et bientôt Wimax, par des petites cartes de mémoire externe, par une connexion avec un ordinateur..) .

Les données reçues ou envoyées peuvent consister en voix, messages écrits (SMS), fichiers images joints (MMS), e-mails, clips vidéo en direct ou en léger différé, musique, télévision, localisation GPS, contenus de sites Internet, VOIP (voix passant par le protocole Internet) données d'un Intranet d'entreprise et, nous l'avons vu, maintenant flux financiers. De plus, avec des systèmes comme Symbion, ou Windows version Ce ou ultérieure, le téléphone mobile n'intègrent plus les fonctions d'un PC ; il devient un PC.

Ce qui en fait doublement une cible pour la cybercriminalité

Sur les ordinateurs « classiques », celle-ci est capable de réaliser ces performances qui se transposent dans le domaine du GSM :

- Prélever de l'information non autorisée

- Saboter des données, des systèmes et des fonctionnalités (éventuellement en vue d'un chantage), par via un logiciel malveillant

- Commander l'appareil à l'insu du propriétaire, lui faire réaliser des opérations, voire dépenses injustifiées (appel de numéros surfacturés), la compromission d'autres cibles, des attaques en réseau contre des cibles

- Falsifier : persuader le propriétaire légitime que tel document ou programme émane d'une personne ou d'une organisation pour l'amener à livrer ses secrets, à se mettre en position de faiblesse, à réaliser des actes qui se retourneront contre lui

Des forteresses aux multiples brèches

Par définition, le téléphone mobile est même encore plus fragile qu'un ordinateur :

- Il n'y a guère de culture de la sécurité sur les mobiles. A fortiori pas d'équivalent de tout le marché des logiciels et entreprises de sécurité informatique, ni des réseaux d'entraide entre utilisateurs pour s'informer des derniers dangers et de leurs remèdes.

- Dans le cadre d'une course aux prix et aux nouvelles fonctionnalités, les fabricants ont mis l'accent sur la découverte du nouveau standard ou des nouvelles adjonctions bien plus que sur la sécurité.

- Le téléphone mobile, par définition transporté avec soi, est par nature plus facile à voler ou à manipuler physiquement. Certes, il est défendu par un code et par des cartes (SIM et IMEI), mais ce n'est guère un obstacle pour un délinquant organisé qui sait les déplomber ou les falsifier

- Le téléphone mobile est une forteresse qui a de multiples portes, en l'occurrence des ports correspondant chacun à une forme d'émission ou de réceptions. Et physiquement et du point de vue logiciel, il est traversé par des flux qui parviennent des réseaux GSM, des ondes de Bluetooh, de celles du Wifi, d'Internet… et qui représentent autant de dangers. Certains de ces systèmes sont réputés comme étant des passoires à sécurité.

- Plus le marché et vaste et plus il est standardisé (plus les mêmes systèmes et implémentations touchent de monde), plus la cible est rentable pour un cyberdélinquant.

Par ailleurs, ces dernières années, les affaires touchant à la sécurité des mobiles se sont multipliées. Certaines étaient très « haut de gamme » et visaient par exemple à faire de l'espionnage économique (forcément coûteux) sur les téléphones des responsables économiques ou autres. Mais d'autres s'adressaient en masse à des utilisateurs ordinaires pour leur faire dépenser quelques cents, un petit vol presque invisible sur une facture, mais très rentables pour celui qui en recueille le résultat à grande échelle.

Parmi les nombreuses attaques constatées sur la sécurité des mobiles, on citera :

- Le mailing de masse de « vers » (logiciels malveillants comme VBS/eliles 3) et de SMS malicieux liés des tentatives de phishing (incitant les usagers à aille se faire piéger sur de faux sites)

- Des virus « mixtes » fonctionnant aussi bien sur le Net que sur les mobiles ou la transposition au monde des mobiles des logiciels malveillants qui prélèvent des données sur des PC, en perturbent le fonctionnement, agissent à retardement, des virus, des vers, des « chevaux de Troie » et autres logiciels d'intrusion du même type.

- Des programmes prenant le contrôle des mobiles pour leur faire appeler des numéros payants à l'insu du propriétaire

- De façon plus générale des « élévations de privilège », par lesquelles un manipulateur fait exécuter à un téléphone des fonctions qui devraient être réservées au seul propriétaire légitime Parfois il suffit d'introduire un logiciel vendu dans le commerce comme Flexyspy qui enregistre les numéros appelés, le contenu des conversations et des SMS…

- Des opérations physiques sur les téléphones : vol pur et simple bien sûr, mais aussi manipulations à l'insu du propriétaire pour rendre le téléphone plus vulnérable.

- Des interceptions des numéros de codes, soit en enregistrant les touches tapées, soit par des méthodes plus sophistiquées le « *Imsi-Catcher* » : un appareil s'interposant entre le mobile et la borne en prenant la place de la seconde pour intercepter tous les appels avant de les retransmettre au réseau GSM. Le téléphone qui a ainsi accepté l'appareil comme sa station « légitime » n'est plus protégé par un système de cryptologie.

- De multiples cas de contenus illégaux, d'envois non sollicités

- Des intrusions dans les mobiles par Bluetooth ou Wifi pour consulter le contenu des mémoires, intercepter, simuler ou provoquer des communications voire transformer le mobile en micro. Ceci se fait parfois par « war driving », en promenant un scanner dans un véhicule pour rentrer dans les réseaux Wifi vulnérables, par *bluebuggin* pour prendre le contrôle d'un téléphone mobile à courte via Bluetooth (et éventuellement de lui faire écouter les conversations de son propriétaire, même éteint).

- Des scandales d'écoutes illégales de téléphone mobile directement chez l'opérateur : espionnage d'hommes politiques ou de vedettes directement chez Vodaphone en Grèce, et directement chez Telecom Italie chez nos voisins transalpins.

Ajoutons que les attaques contre les systèmes de protection peuvent se faire de multiples façons (sans même parler de la méthode qui consiste à les voler ou à menacer les propriétaires) :

- Via le digicode de l'utilisateur commandant les fonctions bancaires
- Au niveau de l'algorithme d'identification et de l'échange de messages prouvant la possession d'un code
- Par interception du segment radio de la transmission chiffré de façon symétrique avec une clef relativement faible
- En s'interposant entre la station-relais et le récepteur
- en s'interposant par un réseau type Bluetooth ou Wifi
- En falsifiant le TSM (Temporary Mobile Suscriber Identity) qui permet à un téléphone de fonctionner sur divers réseaux, par exemple à l'étranger, sans tout révéler sur son propriétaire
- En s'emparant ou en falsifiant les deux puces d'un mobile (SIM et International Mobile Suscriber Indentity)
- En intervenant au niveau de l'ordinateur de l'opérateur (ou de la banque…)

En d'autres termes autant de possiblités de substitution, de prélévement et d'opérations non autorisées. Mais aussi de prédation et de sabotage pouvant donner lieu à chantage et extorsion. De la mini-ecroquerie pour voler quelques roupies numériques à un malheureux aux grandes opérations coordonnées portant simultanément sur la prise de commande de milliers de comptes : le champ est vaste qui vient de s'ouvrir à l'imagination criminelle. Il couvre aussi bien des actions sophistiquées basée sur la cryptologie que des escroqueries basées sur la naïveté ou la faillibitié humaines.

Conclusion

S'il est un cas où le décèlement précoce doit s'appliquer, c'est bien à celui-là. Nous voyons la conjonction d'une technique encore mal sécurisée, d'une multiplicité de maillons faibles- qu'ils soient matériels ou humains-, d'une dispersion internationale et d'une multiplication des cibles mal protégées, de gros enjeux financiers, de risques minimal et de possibilités d'expansion et de profits grâce aux réseaux pour des organisations travaillant en réseaux. Certes, on se doute que des organismes comme Mastercard qui ont assez payé pour savoir ne vont pas négliger la sécurité. Mais il reste que les problèmes posés par les mandats internationaux virtuels ne se résoudront pas forcément par davantage de protection technologique ou de meilleurs algorithmes : beaucoup seront simples voire rustiques tout en se posant à l'échelle planétaire. Raison de plus pour en surveiller les développements.