

# Comment le spam utilise les failles conceptuelles d'Internet

Par Jean-Marc Dinant

Doctorant en Informatique (Université de Namur)

Expert judiciaire devant les tribunaux

# De l'origine d'internet

- Le réseau était d'abord militaire et résistant aux pannes. Ensuite il est devenu académique. Puis il s'est ouvert au monde.
- Philosophie du global village
- Le protocole HTTP dans sa définition originale prévoyait d'inclure de manière systématique dans l'entête de la requête l'adresse email de l'utilisateur
- Les raisons d'être de la page référente dans chaque requête HTTP sont louables
- Conclusion : pas de sécurité lors de la conception. Failles par effet de bord.

# De l'approche du problème par le droit

- Données nominatives => données à caractère personnel (notion d'identité; qu'est-ce que l'identité ?). Une adresse email de type [sdfge43@yahoo.fr](mailto:sdfge43@yahoo.fr) n'EST PAS UNE DCP. Elle permet de contacter mais pas d'identifier (nuance!)
- Approche par la cybercriminalité
  - Intrusion dans un SI
  - Ecoutes téléphoniques : prendre connaissance du contenu d'une communication (on se moque bien si on peut identifier les personnes)
- Approche spécifique cybermarketing limitée aux DCP (art 14 directive 95/46)
- Attention : possibilité de réguler les ETT prévu dans Directive 2002/58 art 15. et directive 99/5

# D'une approche sociale

- Le citoyen raisonne par comparaison et se base sur des grands paradigmes (le téléphone, la télévision)
- En pratique, il y a l'inversion du paradigme client/serveur. L'internaute fournit de l'information au réseau (cookie). Le réseau peut prendre l'initiative de le contacter. Le visiteur visité. Microsoft Internet Explored
- Disparition progressive et incessante de la maîtrise de l'utilisateur sur le fonctionnement des équipements terminaux de télécommunication (pe batterie d'un GSM).  
Mythe de l'ambient intelligence
- L'apparence ne s'est pas modifiée
- Mythe du « user empowerment »

# De l'approche par l'informaticien

- L'informaticien estime avoir une prérogative de décider qui peut avoir accès (et quel type d'accès (RWXD)) à quelle données ou à quelle ressources
- Il attribue des permissions pour certaines finalités (de manière implicite mais certaine : à certains rôles)
- Il est inconcevable que ce soit la personne qui prend mes données qui puisse lui-même en déterminer la finalité

# D'une approche pragmatique

- Qui décide ce qu'on peut faire de mon adresse électronique. Qu'importe. Mais il faut une rencontre de volonté par rapport au moins à plusieurs éléments:
  - Qui va l'utiliser ?
  - Pendant combien de temps et à quelle fréquence
  - Va-t-on la transmettre (je préfère m'en charger)
  - Pour me transmettre quel type de contenu (volume, fond et forme)
  - Quel est mon pouvoir réel si coup de canif dans le contrat ?
- Il s'agit donc pas de courrier électronique non sollicité ou non désiré mais non conforme par rapport à un engagement/des conditions d'utilisation
- Attention aux engagements tacites

# D'une approche par le bon sens, voire la sagesse...

- Il n'est pas possible de respecter la volonté du détenteur d'une adresse mail s'il se tait. Les cdts d'utilisation doivent accompagner l'adresse mail, être collées à celle-ci ou mieux *être* l'adresse mail elle-même.
- Le pseudonymat a ses limites en termes de gestion par l'utilisateur. Celui-ci doit être aidé. Il faut lui offrir un service de pseudonymat. Son ISP ou un tiers de confiance peut jouer le rôle d'un infomédiaire
- Mieux vaut prévenir que guérir...
- « et s'il n'y a qu'un seul juste dans Ninive, elle ne sera pas détruite...et son serveur SMTP ne sera pas blacklisté »  
(attention au droit de l'expéditeur !!!)

# Les failles de système mail

- L'adresse email est +/- la même pour tous
- L'adresse email est transmissible
- L'adresse email est sans conditions
- L'adresse email peut être forgée
- L'adresse email peut être acquise par un robot
- => Le rêve est donc une adresse email intransmissible, différente pour tous, qui indique ses propres cdt's d'utilisation, non forgeable, révocable et qui ne peut pas être acquise par un robot
- Le tout avec un minimum de contraintes pour l'utilisateur

# Principes de fonctionnement des solutions actuelles

- Filtrage lors de la connexion ou après la réception sur base du contenu ou de l'adresse IP de l'expéditeur. Liste noire, blanche voire grise. Problème de performance, d'engorgement du réseau si filtrage au niveau client, de faux positifs ou négatifs, de violation du droit de l'expéditeur,...

<=>

- Seul un utilisateur peut dire que c'est un spam ... et encore

# Le respect des paradigmes sociaux

- Le courriel est gratuit
- L'identification ne peut pas être tellement forte qu'elle empêche le pseudonymat
- Le spam nait d'un détournement de finalité, c'est cela qu'il faut combattre

# Les principes d'un nouveau type de protection : le « mailmediary »

- Ma nouvelle adresse mail : <http://...>

# Bienvenue sur la page de Pierre Dupont

- L'utilisation de l'adresse mail de Pierre Dupont est sujette aux cdts suivantes : j'accepte les mail non commerciaux relatifs à la lutte anti-spam sur Internet
- Votre adresse ip est 122.23.43.45
- Votre DNS est adsl234.Wanadoo.ma
- Votre adresse email ?
- L'heure actuelle est
- Etes vous d'accord oui ou non ?
- {SNIP}
- Hashing du texte ci-dessus = AD3421FGHJMZCXV4ER32
- Votre adresse pour Pierre Dupont :  
[Pierre.Dupont@AD3421FGHJMZCXV4ER32.imd.org](mailto:Pierre.Dupont@AD3421FGHJMZCXV4ER32.imd.org)
- Les cdts d'utilisation sont sur  
<http://www.imd.org/AD3421FGHJMZCXV4ER32>

# Particularités de cette adresse email

- Elle est « finalisée ». N'importe qui peut connaître ses cdt's d'utilisation qui sont donc opposables
- Elle constitue une preuve électronique raisonnable de l'accord entre les parties (enforcement par contrat, on n'évoque pas la privacy)
- Elle est non transmissible.
- Elle *peut* devenir payante
- Elle identifie de manière raisonnable l'expéditeur (IP+?email)
- Elle est révocable
- Elle est non devinable (att: inclure random dans cdt's)
- Elle est gérable (grâce à l'infomédiaire)
- Elle *peut* être rendue non acquérissable par un automate
- Elle ne présente aucun risque de faux positif (sauf en cas de vol)
- Elle n'entraîne pas le changement d'adresse mail pour les membres de ma communauté
- Elle permet d'empêcher *l'envoi* de spams

# Particularités négatives de cette adresse email

- Elle demeure vulnérable par rapport aux zombies
- La sécurité est orthogonale à la fonctionnalité. La solution est lourde pour le premier contact pris à l'initiative d'un expéditeur extérieur à mon domaine de confiance.
- La solution est lourde pour l'infomédiaire

# Conclusions de cette intervention

- Le seul filtrage légitime (\*) et « sans faille » ne peut s'opérer que sur base des cdts d'utilisation convenues de manière libre et explicite entre l'expéditeur et le destinataire
- Les solutions anti spam doivent être prises en charge par ceux qui en ont les moyens (financiers et techniques). Le filtrage des spammeurs risque de devenir le filtrage des pauvres et des étrangers.
- Une solution antispam globale doit être une surcouche technique de l'infrastructure actuelle qui comporte des failles structurelles.
- Il faut faire preuve de sagesse. L'Afrique ne serait-elle pas en avance ?