Le 25 août 2013

Sécuriser les échanges numériques dans l'espace européen

Après avoir mis en lumière les mécanismes de surveillance des échanges numériques à l'œuvre dans le système PRISM, ce document propose d'engager des mesures techniques destinées à préserver les intérêts des citoyens et des Etats européens.

1/ La surveillance des échanges numériques

L'affaire PRISM a montrée comment les échanges numériques peuvent être surveillés, au motif de lutter contre le terrorisme ou au profit de l'intelligence économique ou politique de certains Etats.

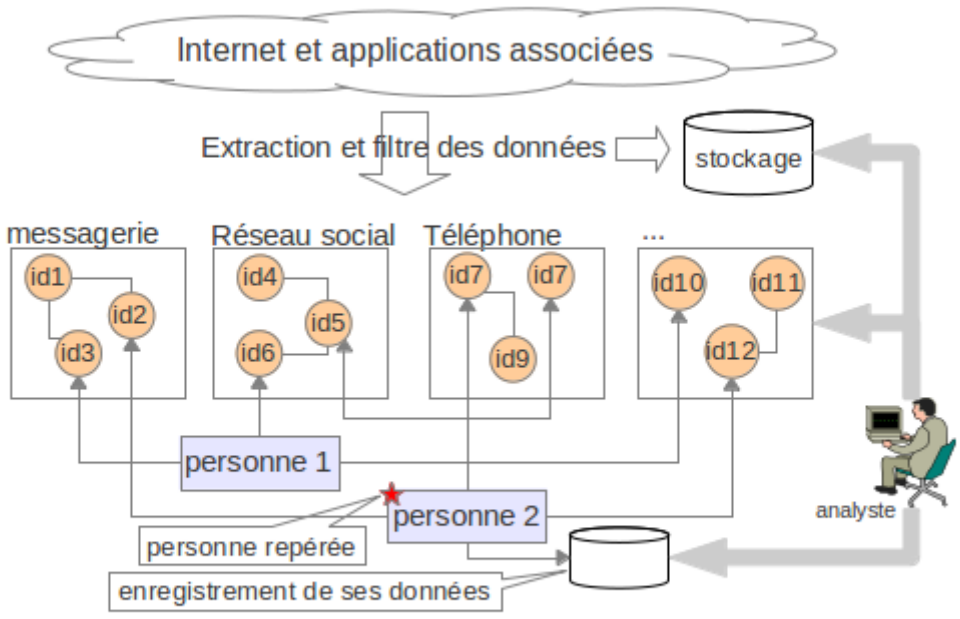
Le recoupement des informations diffusées montre qu'il s'agit probablement :

a) d'abord d'établir le graphe des relations entre les différents identifiants (messagerie, réseaux sociaux, téléphone ...) utilisés par les personnes ;

b) puis de relier ces identifiants à leur propriétaire respectif pour obtenir le graphe des relations entre les personnes ;

c) et d'enregistrer le détail des informations échangées, saisies ou consultées, en isolant celles des personnes repérée comme étant à risque ;

d) le dispositif permettant d'analyser et de croiser l'ensemble des données.



Extraction et mémorisation des relations et des données des internautes

2/ La protection technique insuffisante des données personnelles des internautes

Les données peuvent être captées :

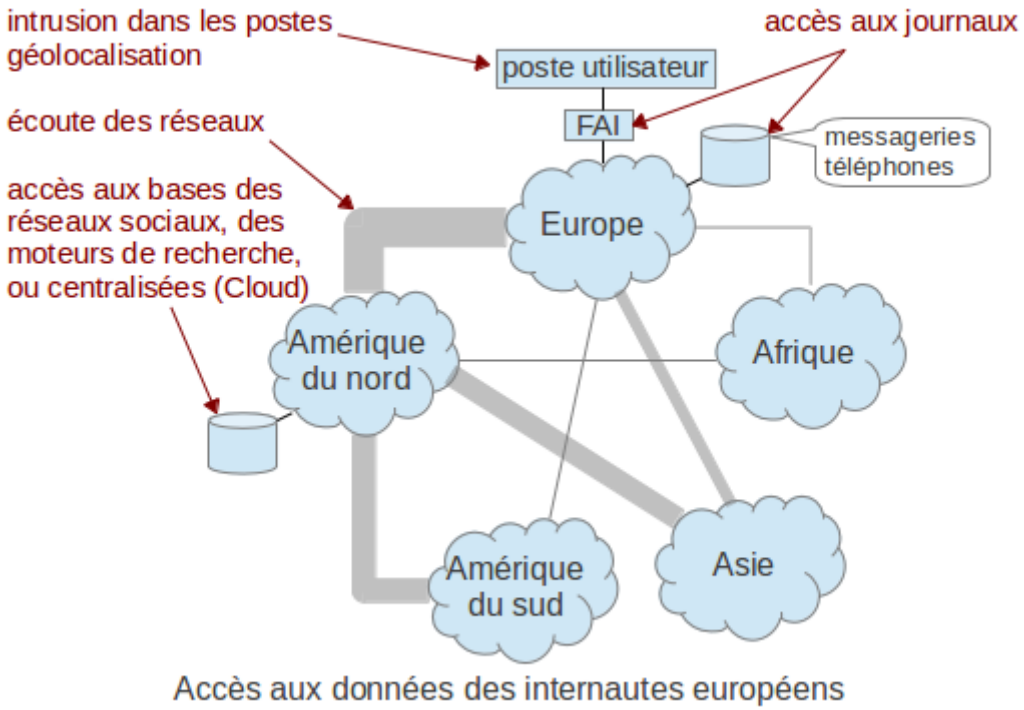
a) lors de leur transmission sur les réseaux, l'existence de points de concentration massifs des échanges (principalement les câbles sous-marins, et dans une moindre mesure les satellites, reliant les continents) le permet, ainsi que l'absence fréquente de chiffrement des données, les méta-données (qui parle à qui) étant généralement transmises en clair ;

b) dans les bases de données des réseaux sociaux, des moteurs de recherche ou centralisées, par les entreprises qui les gèrent mais aussi par les Etats qui peuvent exiger d'y avoir accès ;

c) dans les journaux des fournisseurs d'accès (FAI) ou de messagerie, par les entreprises qui les gèrent, mais aussi par les Etats qui peuvent exiger d'y avoir accès ;

d) dans les postes utilisateurs, où la présence persistante de failles de sécurité dans les logiciels propriétaires qui les équipent, alors que ces failles sont presque absentes des logiciels libres équivalents qui disposent pourtant de moyens bien moins importants, laisse supposer une volonté d'organiser des accès dérobés ;

e) par géolocalisation des terminaux (adresse IP des postes, téléphones mobiles).



Accès aux données des internautes européens

3/ Des mécanismes de protections existants, réservés à des actions militantes

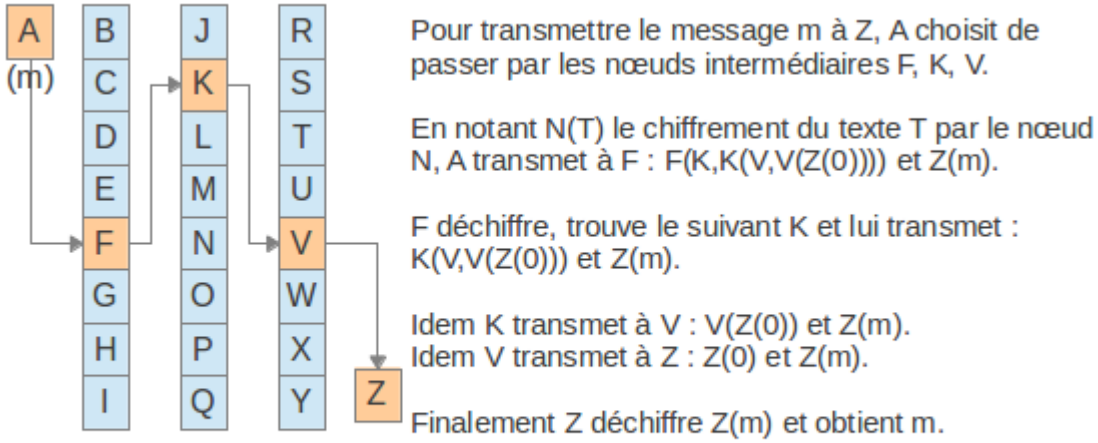
Les mécanismes de protections existants

Différents mécanismes[1] de protection des échanges, des données stockées et des données consultées sur internet ou été mis au point dans les années passées. Ils utilisent principalement deux techniques :

- le chiffrement des données ;
- la passage par des intermédiaires destinés à masquer l'identité de l'internaute.

Le système TOR[2] par exemple utilise ces deux techniques pour réaliser une protection « en pelure d'oignon » des échanges. Il y utilise plusieurs intermédiaires chacun ne connaissant que ses deux voisins pour éviter que la compromission d'une partie d'entre eux ne révèle la chaîne de liaison.

1 http://fr.wikipedia.org/wiki/Anonymat_sur_Internet
2 http://fr.wikipedia.org/wiki/Tor_(réseau)



Principe de la protection « en pelure d'oignon » d'une communication

Dans cet exemple, si K est compromis ou perquisitionné, il lui est impossible de révéler que A a échangé avec Z car il ne connaît que F et V, ni le contenu du message que seul Z peut déchiffrer.

Le système TOR évite l'écoute des réseaux (2a), les données étant chiffrées et les méta-données étant ramenées à celles des machines intermédiaires (nœuds) dialoguant de proche en proche, ainsi que pour la même raison celles des journaux (2c). Mais n'évite pas la captation des données des réseaux sociaux (2b), ni l'intrusion dans les postes (2d) ou leur géolocalisation (2e). Il offre donc une confidentialité ne répondant que partiellement à la captation des données des internautes.

Une logique d'anonymat absolu qui cantonne ces systèmes de protection à un usage militant

Les dispositifs de protection existant ont très généralement suivie une logique d'anonymisation maximale destinée à des personnes ne pouvant ou ne voulant se fier ni aux Etats ni aux fournisseurs des moyens de communication. Ils ont ainsi écarté ou fortement réduit la journalisation des échanges et l'authentification, celles ci pouvant être utilisées à posteriori par les autorités pour retracer l'échange et le cas échéant des données transmises.

Cette approche indispensable pour protéger les actions militantes d'opposants politiques ou syndicaux qui peuvent être confrontés à la répression de leur pays d'origine, ou pour protéger des sources journalistiques, doit à ce titre être impérativement préservée. Mais, il semble qu'elle conduise aussi à constituer un espace d'anonymat total permettant à des activités criminelles de s'y développer[3] sans que les autorités et les gestionnaires de ces dispositifs puissent exercer la régulation nécessaire. Malheureusement, ceci les cantonne à un usage militant et interdit leur généralisation.

4/ Engager un programme européen de protection des échanges

L'Union Européenne ne peut pas rester inerte face à la révélation d'écoutes massives de ses communications qui mettent en péril sa souveraineté et ses intérêts économiques sans perdre l'estime d'elle même. Ni se limiter à des interdictions juridiques dont l'effet est manifestement insuffisant. Il lui faut engager et financer un programme visant à mettre en place les mesures techniques permettant de protéger effectivement les données de ses citoyens et de ses Etats. A défaut un groupe de pays volontaires dont la France pourrait en prendre l'initiative.

En s'appuyant sur l'expertise de personnes qui sont à l'origine ou qui ont contribué à la réalisation

3 www.pcinpact.com/news/81478-ovh-interdit-tor-au-meme-titre-que-tous-systemes-danonymisation.htm

des systèmes d'anonymat existants, ce programme pourrait :

a) identifier les modules à réaliser pour couvrir les différents besoins de protection (2a ... 2e) ;

b) déterminer comment concilier l'anonymat le plus large possible et la régulation permettant d'éviter une présence sauf résiduelle d'activités criminelles, une démarche pragmatique privilégiant l'anonymat pour ne le limiter le cas échéant qu'en dernier recours s'impose afin de préserver les libertés et les avantages du développement des communications ;

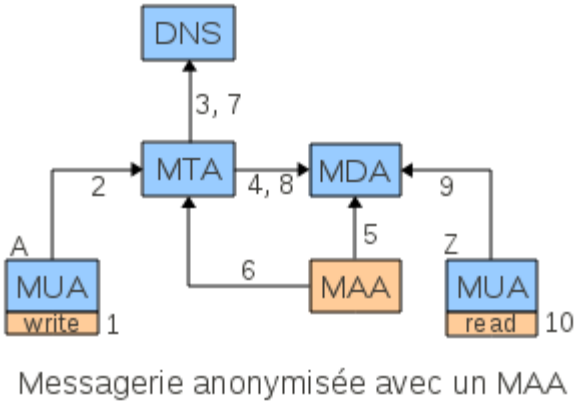
c) réaliser par étapes ces modules, et favoriser leur généralisation par des accords avec les FAI et les prestataires concernés.

La messagerie est un des premiers sujets à traiter compte tenu de la place centrale qu'elle occupe dans les échanges. L'ébauche de solution en annexe illustre ce qui pourrait être fait pour protéger les messages sans bouleverser les mécanismes en place.

ooo00ooo

Le scandale PRISM donne à l'Union Européenne l'occasion de montrer qu'elle est en mesure de s'organiser pour défendre les intérêts de ses citoyens en engageant un programme de sécurisation des données numériques respectueux des libertés. La protection des messageries pourrait constituer la première étape de ce programme.

Annexe
Exemple de sécurisation de la messagerie
utilisant le principe de la « pelure d'oignon »
et s'inscrivant dans les mécanismes existants



Messagerie anonymisée avec un MAA

En bleu les modules existant. En jaune ceux à réaliser.

MUA (mail user agent) : logiciel utilisateur permettant de rédiger, d'envoyer et de recevoir les messages.

MTA (mail transfer agent) : logiciel transférant les messages au serveur du destinataire.

DNS (domain name system) : donne l'adresse d'une machine, le serveur de messages du destinataire dans ce cas.

MDA (mail delivery agent) : serveur de messages du destinataire.

MAA (mail anonymizer agent) : module d'anonymat, à réaliser.

write, read : fonctions d'écriture et de lecture des messages sécurisés, à ajouter aux MUA.

	Etapes d'envoi d'un message sécurisé de A vers Z
1	Mise en forme du message sécurisé : - choix du (ou des) MAA - chiffrement du message: Z(message + objet + émetteur=A) - chiffrement du chemin vers le destinataire : MAA(Z,Z(0))
2	Envoi du message au MAA selon le protocole usuel (SMTP).
3	Résolution de l'adresse du MAA selon le protocole usuel.
4	Transfert au serveur de messages du MAA selon le protocole usuel.
5	Lecture du message par le MAA selon le protocole usuel (POP, IMAP). Déchiffrement du destinataire suivant : Z.
6	Envoi du message au destinataire Z selon le protocole usuel (SMTP).
7	Résolution de l'adresse de Z selon le protocole usuel.
8	Transfert au serveur de messages de Z selon le protocole usuel.
9	Lecture du message par son destinataire Z selon le protocole usuel (POP, IMAP).
10	Déchiffrement et affichage du message reçu.