Autodéfense numérique (sur Internet)

Marc SCHAEFER

19 novembre 2013

Résumé

Lorsque l'on butine sur Internet, on laisse des traces. Cette présentation a pour objectif de sensibiliser à ce problème, puis de donner des pistes pour y remédier.

1 Cette présentation

Autodéfense numérique

Marc SCHAEFER

HE-Arc Ingénierie / ISIC

2 Plan

- peut-on nous suivre, et si oui comment ?
- est-ce un véritable problème ?
- la surveillance étatique ("légale")
- qu'est-ce qui produit ces traces ?
- comment se positionner ?
- des solutions
- des références

3 Peut-on nous suivre sur Internet ?

savez-vous si vous êtes tracé sur Internet ?

avez-vous des exemples où vous vous sentez tracés ?

3.1 Notes

par exemple

- navigateur trop bavard
- suivi par adresse IP (IP tracking)
  - ce billet coûtait moins cher ce matin
  - cette vidéo n'est pas disponible depuis la Suisse
- suivi par accès de ressources
  - démo avec le plugin Collusion/Lightbeam (Mozilla Firefox, Google Chrome, Microsoft Internet Explorer)
    - http ://www.google.ch/ , http ://www.he-arc.ch/ , http ://www.rue89.com/ , http ://www.rtsinfo.ch/
- suivi par cookie (n'importe quel réseau de site coopérant, p.ex. publicitaire)
  - comment http ://www.youtube.com/ sait-il que j'aime Star Trek, alors que je ne suis pas loggué ?

- suivi par login (facebook, google, ...)
  - bouton "J'aime" sur un site tiers
- spam sur vos e-mails (eh oui)

4 Est-ce un problème ?

contre-arguments
- je ne suis pas un pirate !
- qui s'intéresserait à moi ?

faux !
- application
  - existante universelle : publicité contextuelle
  - potentielle : recoupements de bases de données
- impact fort : une fois une information sur Internet, quasi impossible de l'enlever !

existe déjà dans le monde "réel"
- base de données des mauvais payeurs (on y entre aussi par erreur)
- listes noires de divers types

5 La surveillance étatique en Suisse

- la loi suisse sur la surveillance des télécommunications (en évolution) protège le secret (postal) des communications
- ... mais simultanément donne le droit, sur demande judiciaire, à toute écoute électronique

en plus
- les fournisseurs doivent conserver les logs des transactions (pas du contenu) 6 mois
- certains fournisseurs conservent une partie du contenu

et mondialement ?
- PRISM est en fait, une bonne nouvelle

5.1 Notes

PRISM est une bonne nouvelle
- la NSA (et tous les services de renseignement) nous écoutent (on le savait ...)
- la bonne nouvelle
  - la NSA semble avoir besoin de requêtes judiciaires (nombreuses) et de placer des boîtier d'écoute dans la partie non-chiffrée des fournisseurs de contenu (Google, Facebook, Microsoft, Apple, etc)
  - donc ils ne savent pas déchiffrer en masse !
- le problème est le délai de rétention
  - Europe : à limiter
  - USA : pas de droit à l'oubli envisagé, et du stockage en masse par la NSA (décryptable dans le futur !)

6 Qu'est-ce qui produit ces traces ?

Discussion

6.1 Notes

Naviguer, butiner, browser, cliquer, consulter ses e-mails, c'est :
- échanger des datagrammes IP, donc au minimum donner son adresse IP
- résoudre des noms : produire des requêtes DNS (et les entrées de cache correspondantes)
- créer des journaux sur les serveurs concernés , pas forcément bien protégés
- créer des sessions sur des serveurs (référencées par des cookies , des super-cookies voire des Flash cookies)

ainsi que :

- être loggué sur des systèmes d'identification distribués (Google, Microsoft, Facebook, ...)
- éventuellement accéder des ressources qui donneront des informations à des attaquants spécifiques
- souvent en plus tout se passe en clair
  - particulièrement grave p.ex. sur un wifi mal sécurisé (WEP ou WPA2 Personal avec une seule passphrase partagée)
- utiliser des logiciels
  - non authentifiés (sans signature électronique valable), sans commentaires positifs
  - fermés (dont les principes d'action sont secrets)
  - financés par la publicité (vous êtes le produit)

7 Comment se positionner ?

- analyse risque/mitigations
- cette analyse dépend de chaque personne

exemple :
- Mme Martin, employée de la multinationale de l'agroalimentaire Standard SA, poste régulièrement des commentaires privés sur des blogs (en particulier sur les OGM). Elle envoie aussi des documents bancaires scannés à son fils en Australie par e-mail
- recommandations
  - séparer strictement vie privée de vie professionnelle
  - en particulier ne jamais aller sur un blog au travail
  - si sur le même ordinateur, séparer en deux sessions "travail" et "privé" (ou au minimum utiliser la navigation privée), dont aucune n'est administrateur
  - avantage à poster sous un pseudonyme, créer une adresse e-mail pour le privé
  - chiffrer de bout en bout les e-mails contenant les documents bancaires scannés (ou tous !) avec p.ex. Enigmail pour Thunderbird, effacer les documents dès qu'envoyés, si ces documents sont très importants, travailler sur une 3e session

7.1 Notes

plus en détail :

1. définir mes risques particuliers
   - ce que je veux garder pour moi
   - ce que je veux partager, mais dans quells limites
2. définir mon (ou mes) profil(s) d'utilisation des outils informatiques
   - besoin d'immédiateté, de connectivité permanente ?
3. faire l'inventaire des "agents" (logiciels) et services utilisés et de leur configuration
4. définir les risques encourus
   - dépendances aux services Internet hébergés hors du territoire suisse ? (lois étrangères sur la rétention d'information)
5. mitiger (limiter) ces risques
   - confiner
   - rationnaliser l'utilisation des outils et services, "opt out"
   - installer des logiciels anti-tracking (mais attention !)

8 Des solutions (1)

utilisateur
- accéder toujours les versions chiffrées/authentifiées des services (HTTPS) et se délogguer
- mode "surfer sans trace" (navigation privée), mais !
- séparer les activités (une session "travail", une session "butinage"), évt. avec des e-mails jetables

– utiliser un moteur de recherche en SSL avec des garanties de privacité .. ou confiner les recherches (p.ex. dans Wikipedia)
– chiffrer les données de bout en bout (p.ex. avec GPG pour l'e-mail, VPN) plutôt que seulement du client au serveur
– éviter d'activer le flash en permanence (Firefox : Flashblock)
– filtrer les publicités (Firefox : Adblock), gérer les cookies et le Javascript spécifiquement
– mettre à jour les logiciels, faire des sauvegardes et autres recommandations classiques *insuffisantes* (anti-virus, anti-spyware, firewall, ...)

9 Des solutions (2)

administrateurs (d'une entreprise p.ex.)
– préinstaller des logiciels sûrs, produisant le moins de traces possibles
– proposer un proxy qui anonymise les traces, tout en rendant possible l'identification judiciaire par ses propres journaux (p.ex. privoxy), voire en plus un anonymiseur d'adresse IP (tor) dans des cas extrêmes

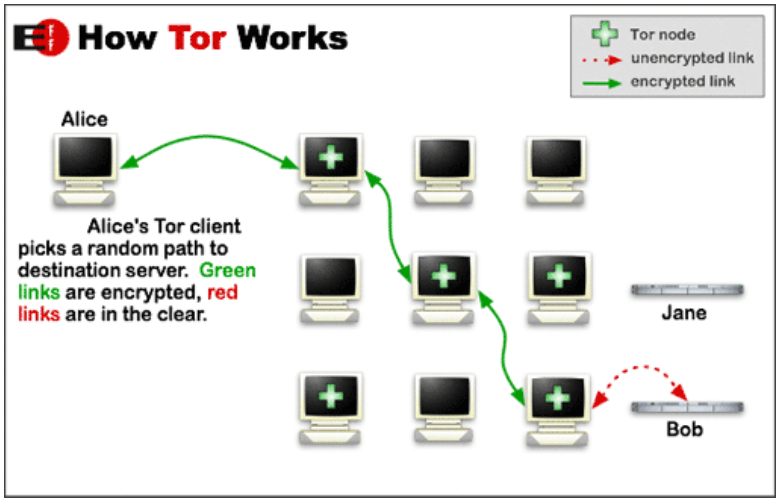
10 Des solutions (3)

développeurs
– assurer que les journaux ne sont pas publiquement accessibles et une politique d'archivage-effacement.
– permettre de se délogguer facilement
– informer de quelles informations sont traitées
– assurer la sécurité des applications Web
la loi
– les adresses IP sont une information privée – en vrai difficile à assurer
– droit à l'image et à la sphère privée – en réalité, difficile à imposer sur Internet
– loi fédérale sur la protection des données
s'assurer !

11 Un exemple extrême : tor (the onion router)

but : anonymisation de l'adresse IP (et du contenu en partie)

principes
– les navigateurs et autres programmes Internet doivent *tous* passer par un proxy (local)
– le proxy se connecte à un noeud tor d'entrée
– les données circulent dans le réseau tor (entre les noeuds) dans un circuit virtuel établi de manière aléatoire
– les données sortent du réseau tor par un noeud de sortie
– les données sont chiffrées, déchiffrées et rechiffrées par couche (comme un oignon)
– aucun des noeuds tor ne connaît toutes les informations (adresse IP client, adresse IP serveur, contenu) simultanément ; seul le noeud de sortie connaît le contenu.
problèmes
– si le trafic est en clair, l'interception reste possible, en particulier si l'attaquant annonce de nombreux noeuds de sortie tor, ou si les noeuds sont vulnérables à des attaques de sécurité, ou si le client donne trop d'informations (p.ex. entêtes HTTP)
– pas de filtrage des informations du navigateur : il faut combiner à un proxy anonymiseur (privoxy) et du SSL (HTTPS)
– vulnérabilités en cas de requêtes DNS ne passant pas par le tunnel (ou en cas d'applications spécifiques, p.ex. Flash)



(Source : Wikipedia)

12 Autres dangers électroniques

- droit à l'image, sphère privée, protection de la personnalité
- usurpation d'identité
- surveillance comportementale
  - p.ex. IP tracking pour les comportements d'achats
  - traçage de la présence physique
- objets qui ne se comportent pas dans votre intérêt
  - lecteur et DVD Blueray qui révoquent a posteriori des droits d'accès au contenu
  - Amazon qui efface des livres achetés sur votre Kindle
  - logiciel (agent) qui vous espionne ou effectue des opérations à votre insu

13 Références

- Anonymat sur Internet, Martin Untersinger, Eyrolles, ISBN 978-221-213-500-8
- http ://lifehacker.com/5395267/how-to-really-browse-without-leaving-a-trace
- http ://www.privacyfoundation.ch/de/service/browserspuren.html
- http ://www.privacyfoundation.ch/de/service/anonymisierungsdienste.html
- http ://guide.boum.org/
- https ://www.privacyinternational.org/

14 Vos questions

Vos questions ?

15 Remerciements

- licence GFDL, invariants : 1ère page