Surveillance étatique d'Internet
État des lieux et comment s'en protéger ?

SCRT Information Security

SCRT Information Security

Sommaire

Qui suis-je ?

De quoi vais-je parler ?

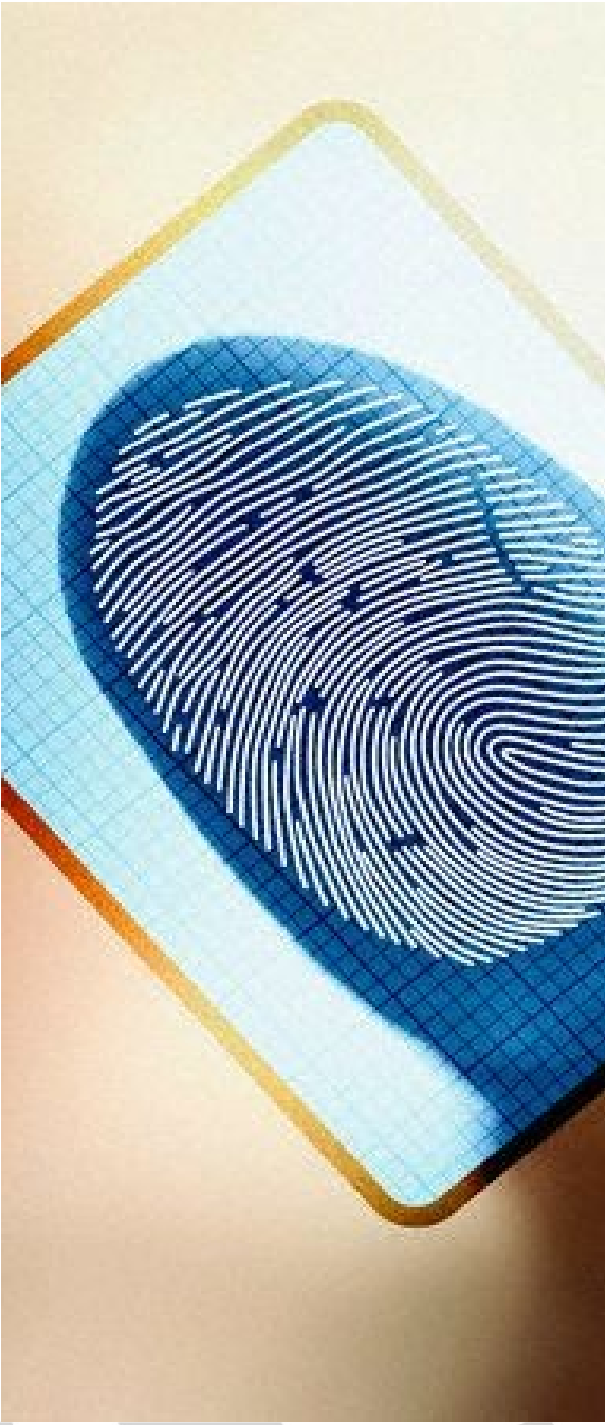
De quoi ne vais-je pas parler ?

Rapide retour sur l'actualité

État des lieux

Mesures de protection

Conclusions



Paul Such / SCRT

- Fondateur de la société SCRT
- Ingénieur en sécurité informatique
- Intervenant dans le cadre de la formation CAS/MAS/DAS
- SCRT : Société Suisse fondée en 2002, basée à Préverenges
  - 12 ans d'expérience
  - 22 personnes
  - 10% des charges annuelles consacrées à la formation des ingénieurs
  - Entièrement dédiée à la Sécurité de l'Information
  - Attaque, défense, investigation, formations
  - Certifiée ISO 27001 dans sa totalité
  - Extrême rigueur dans le traitement des informations reçues
  - Organisateurs de Insomni'hack

SCRT Information Security

YES/NO

De quoi vais je parler ?

- Récentes et (moins récentes) révélations
- Retour sur quelques cas d'actualité
- Etat des lieux
  - Les Etats ?
    - Qu'est ce que cela change ?
    - Qui ?
  - Que sait on aujourd'hui ?
  - Que savait on hier ?
  - Quelles sont les probables possibilités des états
- Comment se protéger ?
  - Mesures techniques
  - Mesures organisationnelles
  - Efficacité probable de ces mesures
- Faut il être paranoïaque ?
- Faut il retourner à l'age de pierre
- Chaque fois que possibe : sources
- La plupart du temps : hypothèses

YES/NO

De quoi NE vais je PAS parler ?

Théories du complot

Politique

Surveillance « physique »

Social engineering

Aspects légaux

BadBIOS :-)

Quantum computing

....

Actualité récente

"Oh, man, the NSA tracks all e-mail, man. They got your cell phone records. They can crack your encryption, man."

« Crazy » people one year ago

"I have uploaded this confidential document on a dropbox share , do you want me to send you a link with my Gmail account " ?

« Crazy » people today

Actualité « récente »

Prism / Snowden

Juin 2013 - Révélations de Snowden

Le grand public découvre que les états ont un pouvoir d'écoute et de surveillance

Ce qui est nouveau (pour le grand public)

- Surveillance non ciblée / collecte d'infos à large échelle au moyen d'Internet
- Prise de conscience

Ce qui ne l'est (pourtant) pas :

- De nombreux pays surveillent leurs citoyens depuis longtemps... (ex : Great firewall of China)
- Autres moyens de collecte/écoute (écoutes téléphoniques, satellite,...)

Sources : Journaux grand public (lematin, 24heures...)

Actualité récente : qu'a-t-on appris

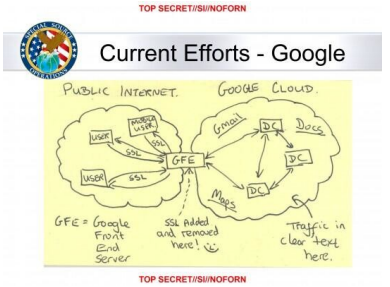
Prism / Snowden

Accès aux données hébergées par Google, Facebook, Microsoft, Yahoo!, YouTube, Apple, Skype

Muscular

La NSA classe des post-its « confidentiels »

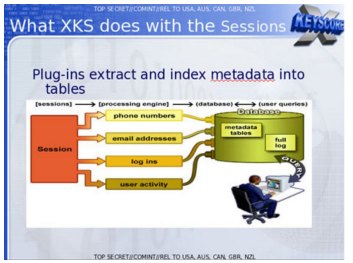
Les données sont aussi collectées sans l'accord des sociétés concernées



Xkeyscore

Collecte et analyse de données utilisateurs à large échelle (formulaires, fichiers envoyés, historique...)

Utilisé par la nouvelle Zélande et l'Australie



Bullrun

Programme commun US-UK (couvert slides suivants)

TOR

Vulnérabilités plugin Firefox

WOW

Infiltration du jeu World of Warcraft

A-t-on vraiment appris quelque chose ?

Enfonçons quelques portes ouvertes...

Les états peuvent demander des informations (voie légale) aux sociétés nationales

… Et les états s'affranchissent parfois des contraintes légales lorsque les intérêts/enjeux sont jugés suffisants

Difficile de savoir qui accède à des données...lorsque elles sont stockées dans le cloud

Il est possible d'intercepter des communications sur Internet (Man in the middle, sniffing...)

Les états font de la recherche dans le domaine de la sécurité (exploit/vulnérabilités)...

Les informations confidentielles ne devraient pas être stockées sur des posts-its

La faiblesse humaine reste une cible de choix

Retour sur quelques cas plus anciens

Flame

Découvert en Mai 2012 (Kaspersky)

600 ordinateurs infectés au Proche-Orient

Première trace d'infection December 2007

20 Mo (!) , interception skype, bluetooth, clavier,...

Grande finesse mathématique/cryptographique

(collisions MD5 -> faux certificat Microsoft)

Evaluation cout développement (source : Kaspersky) :

100 M$

Sources : Wikipedia, Ars technica ,

Retour sur quelques cas plus anciens

Stuxnet

Découvert en Juin 2010

Très probablement développé conjointement par USA/Israel

4 vulnérabilités windows de type 0-day

Attaque relativement ciblée (Siemens, pays)

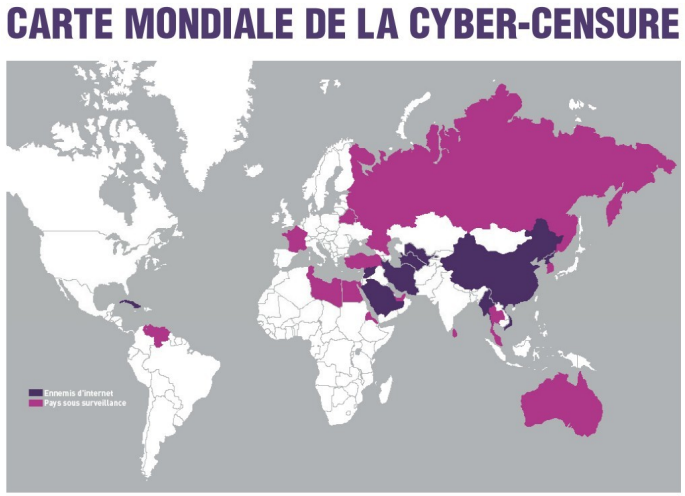
Sources : Wikipedia, Ars technica ,

Quels états font de la surveillance..

Les USA / Israel uniquement ?

Qu'est ce que la surveillance ?

Censure



« Intelligence , cyber-guerre, espionnage... »

- 2008 : création de l'ANSSI en France
- Cas Huawei
- Angleterre , NZ , ...

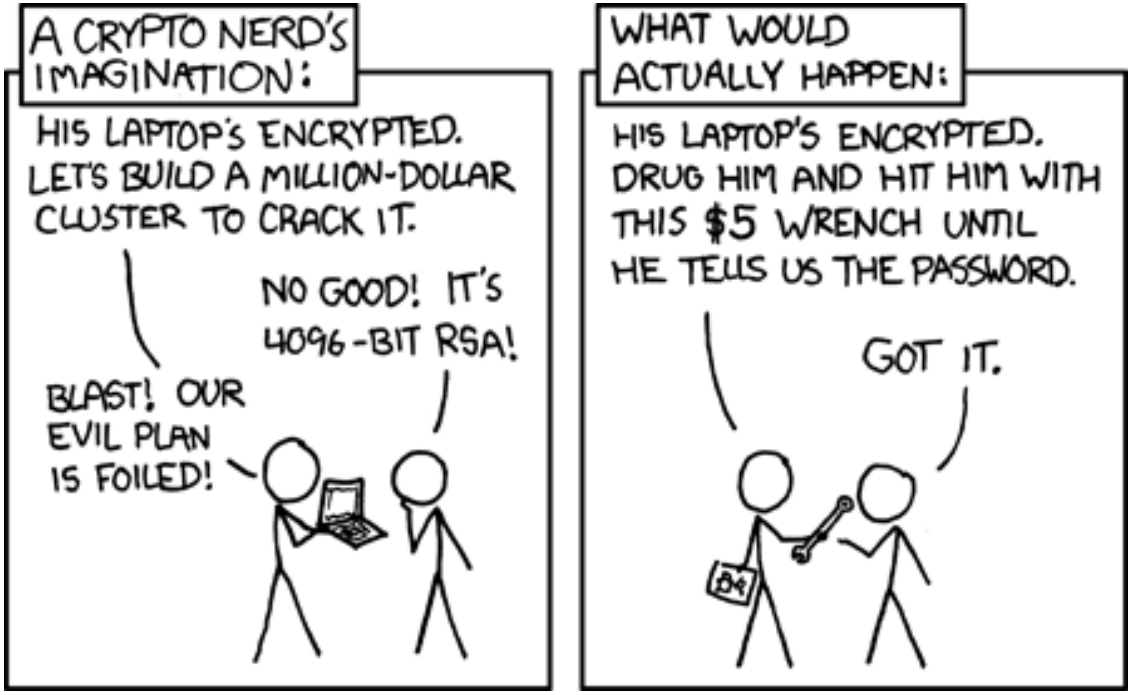
Sources : Reporter sans frontière (2011)

Bullrun

De quoi parle-t-on ?

Programme visant à décrypter les communications (HTTPS, VPN, ...)

La NSA est elle capable de « casser » le chiffrement ?



Bullrun

Donc la cryptographie est inutile et inefficace ... NON !

La cryptographie repose sur des principes mathématiques qui restent (jusqu'à preuve du contraire) dignes de confiance, En revanche...

« Devil's in the details »

Certains standards ont beneficié de « petites » contributions de la NSA

- Exple #1 : En septembre 2013, la société RSA Security a officiellement recomandé de ne pas utiliser ses produits B-SAFE suite à une backdoor (NSA) dans le standard Dual_EC_DRBG
- Exple #2 : Personne ne semble savoir comment s'est fait le choix de certaines courbes elyptiques « standard »

Implémentation

La mise en pratique de ces algorithmes est parfois faite de manière erronnée, accidentellement ou non (backdoors) ...

Sources : Bruce Schneier (himself), CoPS 2013 (EPFL)

Bullrun

Gestion des clés et secrets

Nul besoin de casser les maths lorsque l'on a la clé ! Comment casser votre connexion (chiffrée) à un service sensible ?

- Attaque #1 : « casser » la connexion SSL 2048 bits - impossible ?
- Attaque #2 : Installer un malware sur votre ordinateur – facile !
  (par exemple à l'aide d'un e-mail frauduleux)
  Attendre que vous vous connectiez

Compromission de la chaîne de confiance

SSL repose sur une confiance absolue dans les autorités de certifcation.

ANSSI / Google

7 Décembre 2013

Google indique avoir détecté le 3 décembre des certificats électroniques non autorisés portant sur plusieurs de ses domaines.

Origine des certificats : ANSSI

« Il s'agit d'une erreur dont l'explication a été communiquée à Google »

Sources : http://googleonlinesecurity.blogspot.com.au/2013/12/further-improving-digital-certificate.html

Espionnage/Surveillance

La surveillance par les états repose finalement sur des attaques connues...

... menées à large échelle

Collecte des informtions à la source

Merci le cloud

Ecoutes / interceptions

MiTM . etc...

Chiffrement

2 approches : disposer des clefs , disposer d'une vulnérabilité :

Au niveau du soft, de la machine, de l'algorithme...

Attaque sur le poste

Malware, cheval de troie, ...

La recherche de vulnérabilités reste donc la « clef » principale

-> monétisation et valorisation des attaques de type 0-day

Conclusions / comment se protéger

Comment se protéger ?

Préambule : connaitre le risque et la menace , adapter la réponse

Résultats d'un test d'intrusion / demande de rendez-vous ?

Vaut il mieux héberger son serveur chez soi, chez une PME locale ou chez Google ?

Particulier / Entreprise

Classification des données

Base obligatoire

Conscience

Ce que je fais sur Internet est surveillé par défaut

Facebook, Linkedin, Blog, Twitter...

Comment se protéger ?

Stockage des données sensibles

Pour les données sensibles : stockage "au plus proche" , idéalement chez soi... en respectant l'état de l'art :

- éviter le cloud
- stratégie cohérente (possibilité de s'appuyer sur un référentiel)
- serveurs patchés
- solutions auditées
- isolation/ défense périmétrique
- logs/auditabilité
- chiffrement
- ... bref , ce que vos RSSI essaient de faire depuis des années :)

Limiter le transit des informations

Attention : Internet ne donne pas de garantie sur la route qui sera employée...

Comment se protéger ?

Humain / légal

Bon sens

Formation

Confiance

Contrats

Choix des logiciels/systèmes utilisés

Mauvaises implémentations = danger

Solutions trop propriétaires/trop fermées = danger

Varier/mixer les systèmes (concept de défense en profondeur...)

Comment se protéger ?

Cryptographie

N'est pas la solution à tous les problèmes

Choix des algos utilisés ("Military grade encryption" TM)

Taille des clefs

Autorités de certification

Merci!