

Vie privée et sécurité informatique: enjeux, risques et remèdes

XS

URL pour ces slides

- <https://inda.re/artopie/sectalk1.pdf>

L'histoire d'un "utilisateur lambda"

Nous sommes le 4 Juillet 2014, Boris achète son premier "smartphone". Pour lui c'est le début d'une nouvelle vie. Une vie augmentée grâce aux pouvoirs de communication que son nouvel appareil lui offre. Son frère quand à lui en est déjà à son deuxième acheté. Il faut suivre la mode, une mode dont les rouages, les enjeux, sont hors de portée pour la majorité des adeptes.

On se soucie peu de ce qu'on ne voit pas.



Figure 1: On voit ça, c'est déjà bien assez. *Et surtout c'est cool!*

SST
SST25VF080B
1 MB Serial Flash

SAMSUNG
Application
Processor and
DDR SDRAM

ST MICROELECTRONICS
LIS331 DL
Accelerometer

INFINEON
SMP3i
SMARTi Power
Management IC

SKYWORKS
SKY77340
Power Amp. Module

INFINEON
UMTS Transceiver

**NATIONAL
SEMICONDUCTOR**
LM2512AA
Display Interface

TRIQUINT
TQM666032
WCDMA/HSUPA
Power Amp.

BROADCOM
BCM5974
Touchscreen
Controller

TRIQUINT
TQM676031
WCDMA/HSUPA
Power Amp.

WOLFSON
WM6180C
Audio Codec

TRIQUINT
TQM616035
WCDMA/HSUPA
Power Amp.

NUMONYX
PF38F3050M0Y0CE
16 MB NOR + 8 MB
Pseudo - SRAM

INFINEON
PMB2525
Hammerhead II GPS

LINEAR TECHNOLOGY
LTC4088-2
Battery Charger/
USB Controller

NXP
Power Management

INFINEON
Digital Baseband
Processor



Figure 2: C'est plus accueillant que ce qu'il y a dedans

Nous sommes alors à l'époque d'Android "KitKat", soit 6 ans après la "Révolution" de l'iPhone premier du nom. Android KitKat c'est la version dans laquelle Google introduit une nouvelle fonctionnalité qu'ils nomment alors commercialement "Advertising ID". Sans vraiment en faire la publicité toutefois, c'est juste rajouté au système d'exploitation de l'ordinateur de poche.

- https://en.wikipedia.org/wiki/Advertising_ID

Les fabricants d'ordinateurs de poches connectés et remplis de capteurs, ainsi que les éditeurs de logiciels qui les rendent utilisables ont des objectifs qui leur sont propres, avant tout financiers pour assurer une certaine rentabilité. Ils sont également sous l'influence directe du "progrès technologique" instigué par certains mouvements, la science ou les états et dont les objectifs sont très variés.

Au fil du temps, Boris va se servir de l'appareil qu'il à payé de sa poche, tous les jours, mais également de son ordinateur portable personnel, de l'ordinateur fournit par l'entreprise qui l'embauchera, d'une vingtaine de services en ligne (l'ordinateur et les programmes de quelqu'un d'autre) et parfois, de la console de jeu vidéo qu'il partage avec son frère.

Le pouvoir de l'utilisateur d'un logiciel

Accès au code source

Pour tout programme, il existe un critère fondamental, celui de l'accès au code source authentique de ce dernier.

Pour un utilisateur, la probabilité de connaître le fonctionnement réel d'un programme sans être capable de lire son code source est proche de zéro.

Propriété intellectuelle

Un autre critère déterminant le pouvoir de l'utilisateur est celui de la propriété intellectuelle du code source.

La propriété d'un logiciel détermine qui détient le pouvoir de dicter l'ensemble de son fonctionnement, qu'il produise un résultat visible ou non à l'utilisation.

Contrat d'utilisation

Le contrat de licence d'utilisateur final, aussi appelé conditions générales d'utilisation d'un programme définit un cadre dans lequel l'utilisation doit avoir lieu, d'éventuelles garanties et leur périmètre ainsi que les modalités de support dues ou interdictions relatives à l'utilisation du programme.

On parle aussi communément de "licence" d'utilisation. Ce document n'est pas obligatoire et son contenu est choisi par l'entité qui produit le code source.

Il peut s'agir d'un contrat rédigé sur mesure et apposé par le propriétaire lors de l'utilisation d'un programme, voir d'un ensemble de programmes qu'il faut accepter de manière interactive ou tacite. Ce qui permet aussi à l'éditeur de se dédouaner légalement de tout usage malveillant de la part de l'utilisateur.

Ou bien d'une licence pré faite choisie par le créateur du programme qui va déterminer les droits des utilisateurs à sa publication. C'est dans ce cas ci, généralement une licence toute faite parmi les licences de logiciel libre existantes.

Libertés relatives aux programmes

La licence choisie par le créateur du programme définit également les libertés conférée lors de sa publication.

Dans le cas des logiciels libres, une licence définit les libertés qu'on tous les individus disposant d'une copie du code source.

On retrouve généralement un ensemble parmi les libertés suivantes:

- lire et étudier le code source
- modifier le code source
- utiliser le programme résultant du code source
- redistribuer le code source modifié
- ne pas être dans l'obligation de mentionner l'origine du code source

Le pouvoir de l'utilisateur d'un ordinateur

La garantie légale de conformité

La garantie légale permet au propriétaire du bien de réclamer sa réparation ou son remplacement en cas de problème qui surviendrait par le cadre défini par le fabricant.

Choix du système d'exploitation

Malgré le problème de la vente liée présente sur certains produits, il devrait être possible pour l'utilisateur d'un ordinateur de choisir les programmes qui y sont exécutés, y compris l'un des plus essentiels: le système d'exploitation.

Choix des firmwares

Généralement plus délicat à remplacer, les firmwares sont fournis par les fabricants des composants d'un ordinateur. Certains firmwares libres existent et peuvent être installés sur les composants compatibles.

Neutralité du réseau

Principe devant garantir l'égalité de traitement des flux de données qui exclut toute discrimination entre la source et la destination.

- https://fr.wikipedia.org/wiki/Neutralit%C3%A9_du_r%C3%A9seau
- https://en.wikipedia.org/wiki/Net_neutrality_by_country
- <https://www.arcep.fr/nos-sujets/la-neutralite-du-net.html>
- <https://www.laquadrature.net/2010/04/13/garantir-la-neutralite-du-net-cartes-sur-table>

Neutralité des terminaux

Les appareils destinés aux utilisateurs doivent, intégrant le réseau, garantir un niveau de neutralité adéquat pour éviter des censures appliquées localement.

Surveillance des réseaux

Le filtrage et l'analyse des réseaux, par certains procédés comme la "Deep Packet Inspection" donnent un pouvoir de censure aux opérateurs et aux états faisant appliquer leur règles.

- https://www.qosmos.com/wp-content/uploads/qosmos_deep_packet_inspection_characterization.pdf

Opérateurs

Les opérateurs privés peuvent être tentés d'utiliser la surveillance du réseau pour mettre en place:

- De la publicité ciblée
- Une qualité de service variable
- Un filtrage empêchant certaines applications de fonctionner

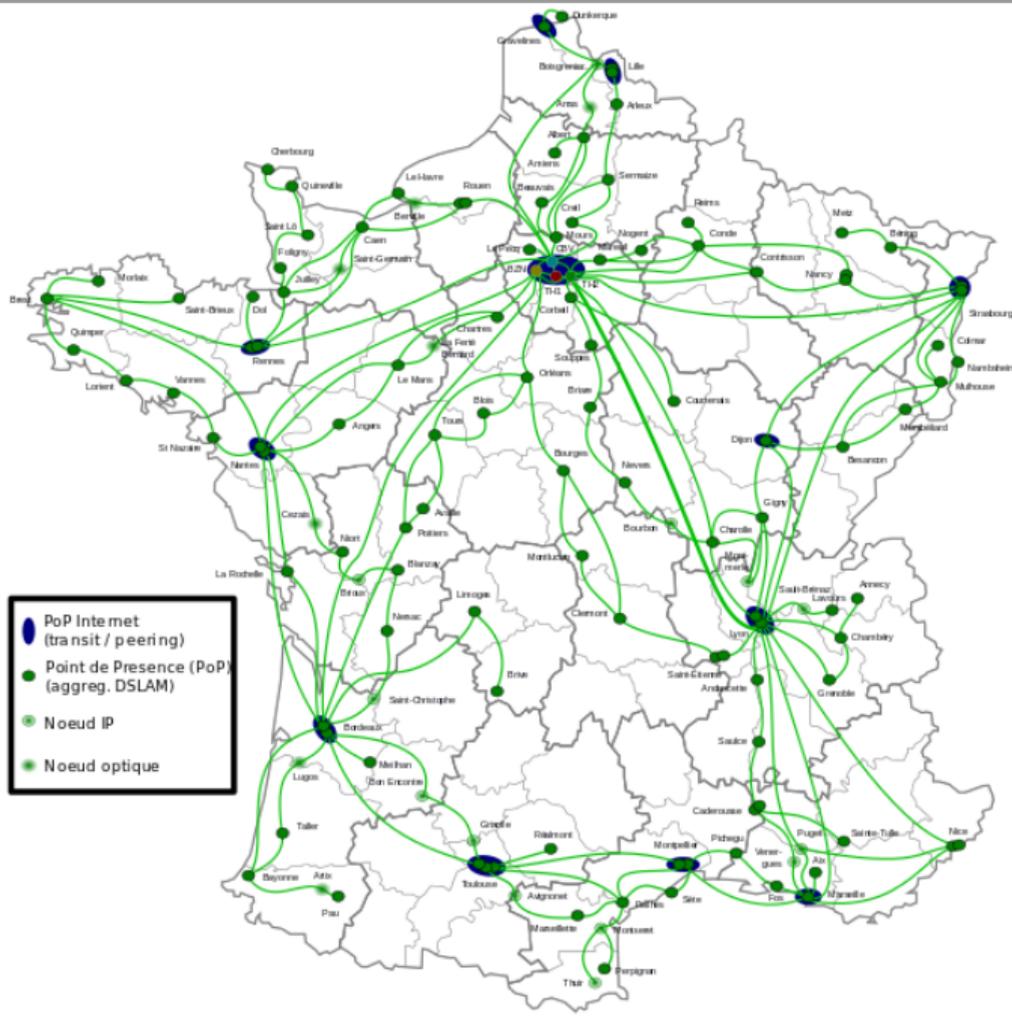
Étatique

En imposant des règles aux opérateurs, les états peuvent interférer avec la neutralité du réseau pour leurs abonnés, notamment pour:

- Repérer des activités jugées malveillantes
- Interdire tout ou partie du trafic selon l'origine ou la destination
- Collecter l'activité des utilisateurs

Structure d'Internet

- Ensemble de protocoles
- Systèmes autonomes
- Passerelles
- Autorités de régulation (ARCEP en France)
- Opérateurs
- Transitaires



Protocoles

Les protocoles utilisés pour faire fonctionner internet et le rendre utile sont nombreux. Ils sont organisés en couches superposées et fonctionnent grâce aux protocoles régissant les couches inférieures.

Les communications physiques entre les équipements (cartes réseaux, switches, routeurs) sont assurés par les couches basses, proche du matériel.

Les usage applicatifs comme le transfert de données reposent sur les couches hautes.

On distingue certains protocoles de bas niveau spécifiquement conçus pour les réseaux locaux ou LAN, “Local Area Network” et d’autres conçus pour les réseaux WAN, “Worldwide Area Network”.

- <https://sebsauvage.net/comprendre/tcpip/protocols.pdf>

Modèle OSI

“Open Systems Interconnection” est le modèle de communication utilisé par internet. Il représente l'organisation en couches des protocoles.

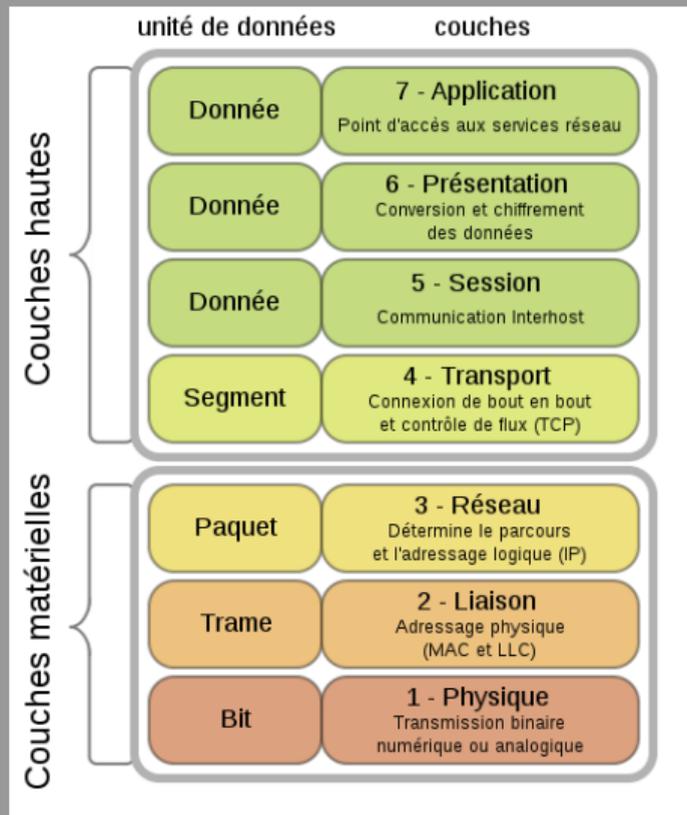


Figure 4: Modèle OSI

ARP

Dans un réseau, l'“Address Resolution Protocol” permet la découverte des adresses MAC, “Media Access Control”, une adresse matérielle unique identifiant une interface réseau et la liaison avec l'adressage IP.

Pour chaque interface réseau, une adresse MAC est assignée par le firmware de la carte réseau, mais il est possible d'en utiliser une autre à partir du système d'exploitation. C'est ce qu'on appelle le “MAC Spoofing”.

41:7D:13:08:92:D4 # Adresse MAC aléatoire

IP

L'IP est responsable de l'adressage des appareils communicants, si une route existe entre deux adresses alors les applications pourront utiliser ces adresses.

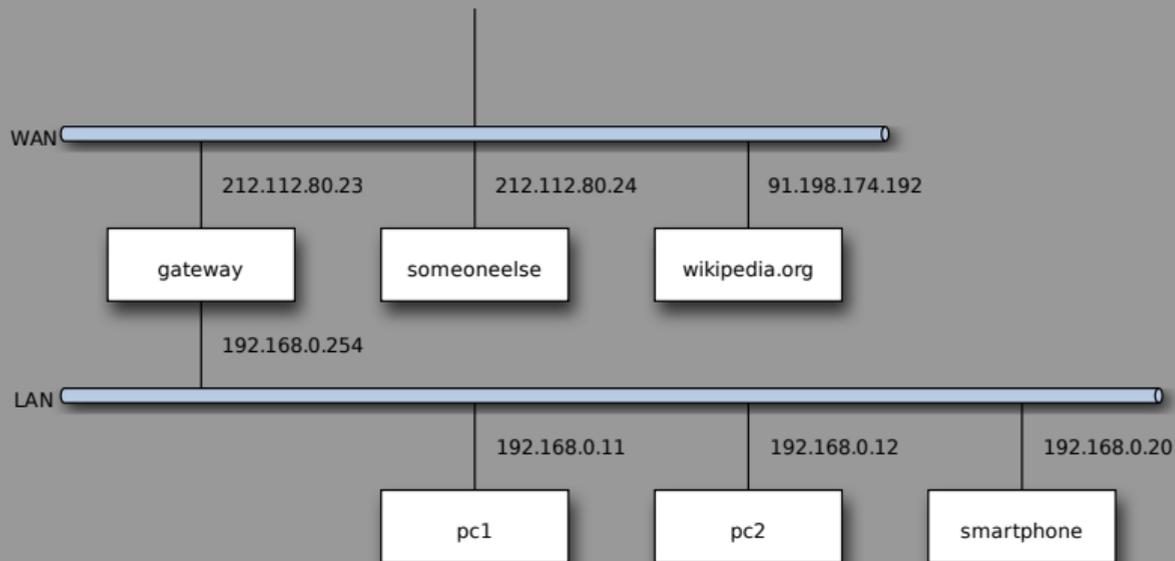
L'adressage consiste à choisir les adresses IP associées interfaces réseaux utilisées, de façon manuelle ou automatique.

L'adressage s'effectue au sein de "blocks IP", représentant l'appartenance à un réseau publique ou privé.

127.0.0.0/24 # IPv4 Class C special IP range
192.168.0.0/24 # IPv4 Class C private IP range
10.0.0.0/8 # IPv4 Class A private IP range

- <https://www.meridianoutpost.com/resources/articles/IP-classes.php>
- https://en.wikipedia.org/wiki/Reserved_IP_addresses

Exemple d'un réseau local (LAN) domestique typique



TCP

Le "Transmission Control Protocol" permet la transmission fiable d'un flux d'octets entre les applications communicantes sur un réseau IP.

(i/e)BGP

“Border Gateway Protocol” est utilisé au sein des AS (interior) ou en périphérie pour assurer les échanges entre différents AS (exterior). Il est responsable de l'échange des informations de routes en se reposant sur d'autres protocoles comme l'OSPF “Open Shortest Path First”.

DNS

“Domain Name System” est un protocole permettant la résolution des noms de domaines récursivement et hiérarchiquement. Il permet aux utilisateurs et aux applications de s'affranchir de connaître les adresses IP's des correspondants par un nom d'hôte (de machine), appartenant à un domaine.

`www.wikipedia.org.`

- https://fr.wikipedia.org/wiki/Domain_Name_System

HTTP

“HyperText Transfert Protocol” est l’un des protocoles les plus répandus chez l’utilisateur, il fait partie de l’écosystème du WorldWide Web il permet la publication et l’interaction de données accessibles sous la forme d’hyperliens.

TLS

“Transport Layer Security”. Anciennement SSL, “Secure Socket Layer” est un protocole de chiffrement de communication.

Il vise à fournir confidentialité, intégrité et authenticité entre applications communicants sur le réseau.

Le modèle client/serveur

Le “serveur” est un programme donnant accès à des information ou un service. Il attends les requêtes des “clients”. Ces derniers sont les programmes qui parlent un protocole applicatif donné tel que l’HTTP ou le SMTP.

Isolation et filtrage réseau

Il est possible de mettre en place le nécessaire pour augmenter la protection d'un parc informatique au sein d'un réseau local.

- Règles de routage au niveau de la passerelle (firewalling)
- Isolation physique
- Filtrage DNS
- Filtrage IP

Traçage sur le WEB

L'écosystème web d'un service en ligne typique est composé de:

- Caches et CDN
- Load Balancers
- Serveurs HTTP
- Serveurs d'application web
- Bases de données
- Systèmes d'authentification
- Systèmes de monitoring
- Ressources tierces, libs javascript, polices de caractères, publicités

Chacun de ces éléments peut garder la trace du passage d'un utilisateur, même non authentifié sur le service.

Exemple de logs http

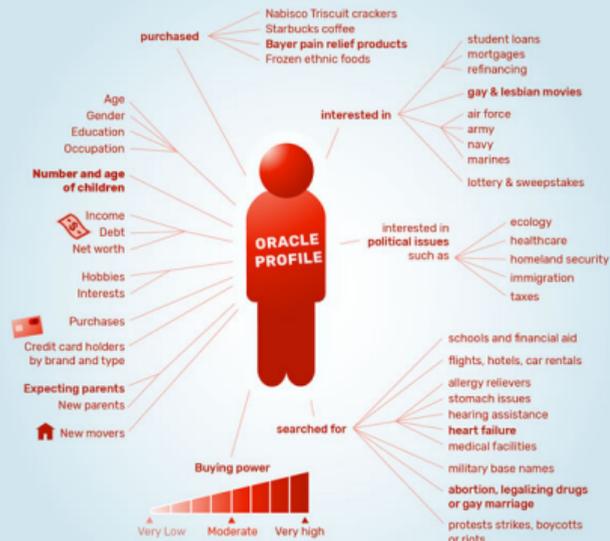
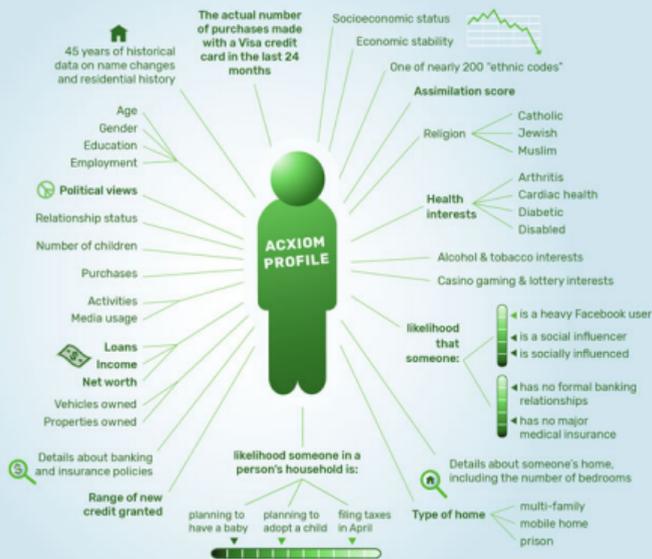
```
inda.re XXX.YYY.ZZZ.FFF - - [04/Jul/2022:23:22:46 +0200]  
"GET /artopie/sectalk1.pdf HTTP/1.1" 200 266963
```

Conséquences pour l'utilisateur

Sans protection adéquate et selon la navigation, les faits et gestes peuvent être enregistrés et réutilisés sans consentement de l'utilisateur.

DATA BROKERS HAVE EXTENSIVE PROFILE INFORMATION ON ENTIRE POPULATIONS

Examples of data on consumers provided by Acxiom and Oracle



© Cracked Labs CC BY-SA 4.0, April/May 2017. Disclaimer: the mentioned companies typically keep information about their activities secret. This illustration is based on publicly available information by Acxiom and Oracle. Every effort has been made to accurately interpret and represent the companies' activities, but we cannot accept any liability in the case of eventual errors. Sources: Acxiom annual reports, developer website (API docs), Oracle press release, help center website, audience playbook, taxonomy updates for January, 2017 (Excel document). For details about the sources see the report "Corporate Surveillance in Everyday Life".

- https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf

Que faire en prévention du tracage sur le web

- Préferer Firefox
- Bien le configurer
- Naviguer sur des sites de confiance
- Utiliser des modules de filtrage
- Et des modules prévenant le “fingerprinting”
- Opter pour des “Frontend” alternatifs aux gros sites

Quelques modules recommandés

- <https://addons.mozilla.org/en-US/firefox/addon/ublock-origin>
- <https://addons.mozilla.org/en-US/firefox/addon/umatrix>
- <https://privacybadger.org>
- <https://addons.mozilla.org/en-US/firefox/addon/noscript>
- <https://addons.mozilla.org/en-US/firefox/addon/happy-bonobo-disable-webrtc>
- <https://addons.mozilla.org/en-US/firefox/addon/font-fingerprint-defender>
- <https://addons.mozilla.org/en-US/firefox/addon/privacy-redirect>
- <https://addons.mozilla.org/en-US/firefox/addon/clearurls>
- <https://addons.mozilla.org/en-US/firefox/addon/cookie-autodelete>

Informations complémentaires

- <https://github.com/intika/Librefox>

Tester les mesures anti-tracage

- <https://coveryourtracks.eff.org>
- <https://browserleaks.com>

Frontends alternatifs

Il existe des logiciels libres hébergés en instances éparpillées un peu partout dans le monde dont le but est de fournir une interface utilisateur à un service tel que YouTube, sans possibilité de tracage vis à vis du fournisseur du service.

- <https://nitter.net> (Twitter)
- <https://libredd.it> (Reddit)
- <https://invidious.io> (YouTube)

Moyens pour lutter contre la censure

Tor

- <https://www.torproject.org>

Proxy HTTP

- <https://www.privoxy.org>

VPN

- <https://mullvad.net>

Traçage par applications android

Malheureusement comme le Web, mais en pire.

- <https://exodus-privacy.eu.org/fr>

Équipements présents sur les smartphones

- Puce baseband
- Gyroscope
- Accéléromètre
- Microphones
- Caméras
- GPS
- Altimètre
- Boussole

Conséquences pour l'utilisateur

Les données collectées dépendent de la ROM, surcouches et applications installées. Généralement il est possible de retracer en détail la vie du propriétaire d'un smartphone qui l'aurait continuellement sur lui.

- <https://www.scss.tcd.ie/doug.leith/privacyofdialerandsmsapps.pdf>

Que faire pour prévenir le tracage sur android

- Opter pour l'utilisation d'une ROM libre
- Favoriser les applications libres
- Filtrer le réseau

Store d'applications libres

- <https://f-droid.org>

Exemples d'applications alternatives

- <https://newpipe.net>
- <https://osmand.net>

Quelques ROMs AOSP

AOSP, pour “Android Open Source Project” est le système de base d’android, par dessus lequel les fabricants et les opérateurs peuvent rajouter des surcouches. Voici quelques systèmes dérivés d’AOSP visant à fournir un écosystème sans trackers imposés de-facto.

- <https://grapheneos.org>
- <https://e.foundation>
- <https://lineageos.org>

Filtrage réseau sur android

- <https://netguard.me>
- <https://trackercontrol.org>
- <https://blokada.org>

Tracage externe

Avec les puces Wi-Fi, Bluetooth ou encore NFC, il est possible de tracker les passants. Il est possible de désactiver ces dernières quand elles ne servent pas.

Attaques sur les services en ligne

Différents scénarios

- Déni de service
- Exploitation d'une vulnérabilité sur un service exposé
- Compromission interne, via un employé par exemple

Conséquences pour les utilisateurs

- Indisponibilité du service
- Vol ou destruction de données utilisateur
- Crackage du mot de passe de l'utilisateur sur le service
- Intégrité des données remise en cause

Vérifier son compte utilisateur

Les attaques réussies sur des services en lignes centralisés sont fréquentes. Grâce aux bases de données des utilisateurs rendues publiques, il est possible de rechercher si des identifiants y figurent.

- <https://haveibeenpwned.com>
- <https://monitor.firefox.com>

Que faire en cas de compromission d'un compte en ligne

- Lister les identifiants utilisant le même mot de passe
- Changer les mots de passes concernés
- Lire les recommandations publiées par le service concerné

Que faire en prévention d'un "Data Breach"

- Utiliser un gestionnaire de mots de passes
- Utiliser une authentification multi-facteurs
- Limiter l'usage de services tiers
- Limiter l'envoi de données personnelles

Gestion des mots de passes et authentification multi-facteurs

- <https://getaegis.app>
- <https://github.com/Kunzisoft/KeePassDX>
- <https://keepassxc.org>
- <https://addons.mozilla.org/en-US/firefox/addon/keepassxc-browser>
- <https://syncthing.net>

Attaques sur un ordinateur personnel

Différents scénarios

- Accès physique non autorisé
- Installation d'un programme malveillant
- Exploitation d'une vulnérabilité locale

Conséquences pour l'utilisateur

- Espionnage et vol de données
- Machine Zombie
- Utilisation des ressources à d'autres fins
- Demande de rançon

Que faire en cas de compromission

- Effacer l'ensemble du système
- Réinstaller ou repartir d'une sauvegarde

Que faire en prévention

- Chiffrer les données localement
- Protéger la chaîne de démarrage
- Mettre en place une sauvegarde régulière
- Connaître le modèle de sécurité de son système d'exploitation
- Vérifier la présence de mises à jour avant l'utilisation
- Assurer une bonne configuration logicielle
- Assurer une bonne isolation des réseaux publiques

Ère du numérique

- Opérateurs des télécommunications
- Fournisseurs de services
- Fabricants
- Exploitants

L'économie de l'information

L'information est traitée en tant que marchandise, capable de générer de la valeur.

- https://fr.wikipedia.org/wiki/%C3%89conomie_de_l'information

Interdépendance des utilisateurs d'un service

Effet de “contagiosité” par lequel les utilisateurs entretiennent collectivement une dépendance au service.

Consentement à la collecte de données

Dans le modèle de consommation actuel, certains acteurs incitent les consommateurs à donner leur consentement pour des collecte d'informations automatiques et régulières.

Hacking Social

Ensemble de techniques dans le domaine de la psychologie visant à orienter les décisions individuelles ou collectives.

Objectifs du piratage

Le piratage est un acte visant à dérober ou rendre inaccessible informations ou ressources informatiques.

Objectifs du hacking

Le “Hacking” est une activité visant à détourner le fonctionnement d’un système pour arriver à une fin non prévue. Sans que cela soit dans un but défini.

Logiciel et Matériel

Bugs

Plus un logiciel est grand, plus la probabilité d'y trouver des bugs est grande. L'ajout de nouvelles fonctionnalités via des mises à jour augmente donc également le nombre de bugs potentiels.

Il est recommandé de se tenir informé des vulnérabilités corrigées sur les logiciels qu'on utilise.

- <https://www.debian.org/security/#DSAS>

Systemes d'exploitation

Ensemble de logiciels responsable de l'interaction avec le materiel.

- <https://www.debian.org>
- <https://www.openbsd.org>
- <https://tails.boum.org>

Bootloaders

Logiciel en charge de vérifier et d'exécuter le système d'exploitation. Le plus souvent fournit avec le système d'exploitation.

Principe de moindre privilège

Principe selon lequel une tâche dispose de privilèges strictement restreint aux besoins de cette dernière.

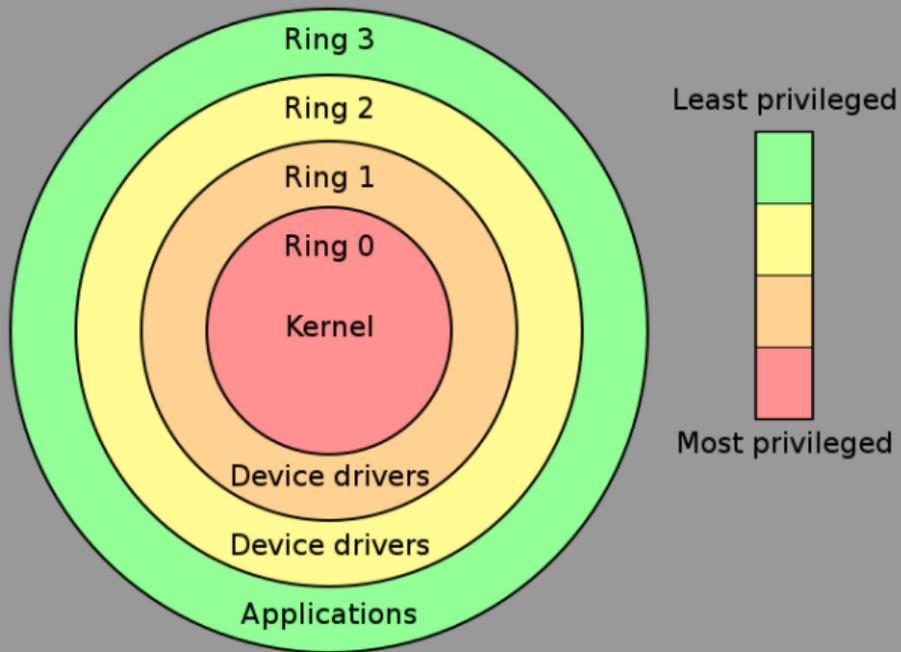


Figure 5: Anneaux de protection x86

Chiffrement des données

Chiffrement matériel

- https://en.wikipedia.org/wiki/Hardware-based_full_disk_encryption

Chiffrement logiciel

- https://en.wikipedia.org/wiki/Linux_Unified_Key_Setup
- <https://en.wikipedia.org/wiki/BitLocker>
- <https://support.apple.com/guide/deployment/intro-to-filevault-dep82064ec40/web>
- <https://nuetzlich.net/gocryptfs>
- <https://gnupg.org>

Autres informations

Dégooglisons Internet

- <https://degooglisons-internet.org>

Site de l'EFF

- <https://www.eff.org>

Hygiène Numérique

- <https://www.hygiene-numerique.com>
- <https://www.hygiene-numerique.org>

Auto-Hébergement “Facile”

“On est jamais mieux servi que par soi même...”

- <https://www.freedombox.org/fr>
- <https://yunohost.org>
- Do it yourself, really

Bonnes pratiques en vrac

- Repérer les mails frauduleux
- Ne pas cliquer sur des liens au hasard
- Favoriser des versions de logiciels stables
- Mettre à jour lors de failles de sécurité
- Y compris le système d'exploitation
- Éviter les échanges non sollicités

On est en 2022

Comment ça sera dans le futur ?