Vie privée et sécurité informatique: enjeux, risques et remèdes V2

xs

URL pour ces slides

- https://inda.re/interhack/sectalk2.pdf

Ancienne version

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

Contexte

Quelques liens pour contextualiser.

Janvier 2024

- ~60 Millions d'utilisateurs d'Internet en France
- ~5,35 Milliards d'utilisateurs d'Internet dans le monde
- ~5,04 Milliards d'utilisateurs de réseaux sociaux
- https://www.statista.com/statistics/262966/number-of-internet-users-in-selected-countries/
- https://www.statista.com/statistics/617136/digital-population-worldwide/

Étude 2023 (Plus company)

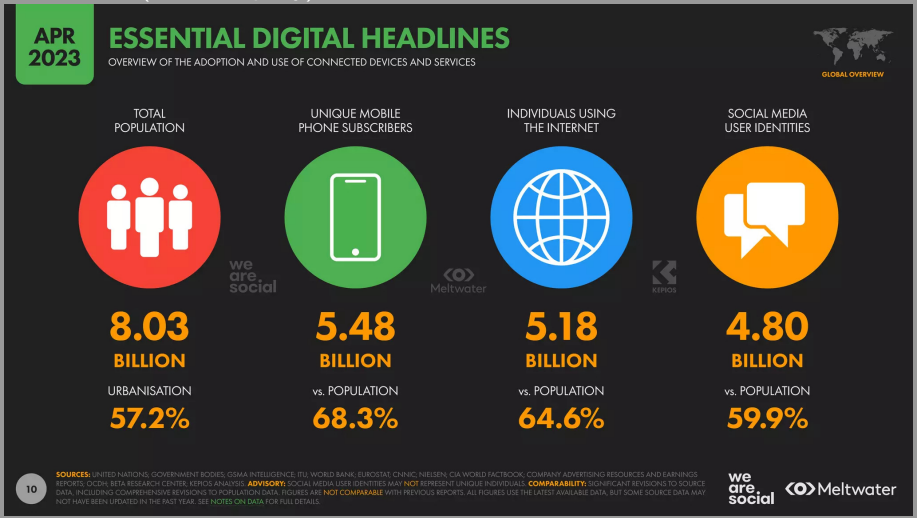


Figure 1: Apperçu de l'usage et de l'adoption d'objets connectés et services

Adverstising ID

Apple, Google et Microsft, opt-out.

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

Communications non sollicitées

- Windows, Linux, OpenBSD: https://0x19.org/posts/2024-02-06.php

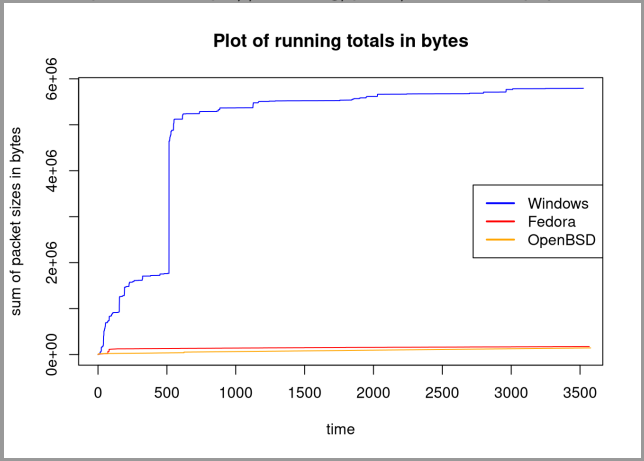


Figure 2: 1h après le démarrage (6MB de données transférées depuis Windows 10)

- Android Mobile OS Snooping:
  https://www.scss.tcd.ie/Doug.Leith/Android_privacy_report.pdf

	Samsung	**Xiaomi**	**Realme**	**Huawei**	**LineageOS**	**/e/OS**	**Google**
Long-lived Device Identifiers	IMEIs, hardware serial numbers	IMEIs, Secure DeviceID, MD5 hash of Wifi MAC address	IMEI, deviceID, guid	hardware serial number, device RSA cert	-	-	IMEI, hardware serial number, Wifi MAC address
Resettable Identifiers Relinkable to Device	Samsung Consumer ID, Firebase IDs	VAID, Google Ad ID	VAID, OAID, device_id, registrationId, Google Ad ID, Firebase IDs	-	-	-	AndroidID, Google Ad ID
Third-Party System App Data Collectors	Google, Mobile Operator, Microsoft, LinkedIn, Hiya	Google, Mobile Operator, Facebook	Google, Heytap	Google, Daily Motion, Avast, Qihoo 360, Microsoft	Google	-	
Main Telemetry Collectors (By Data Volume)	Google, Samsung, Microsoft	Google, Xiaomi	Google, Heytap	Google, Microsoft	Google	-	
Loggers of App Usage Over Time	Samsung	Google, Xiaomi	-	Google, Microsoft	-	-	
Loggers of Apps Installed On Handset	Google, Samsung	Google, Xiaomi	Google, Realme, Heytap	Google, Huawei	Google	-	

Figure 3: Collection de données par variants d'android

- Google Dialer and Messages apps:
  https://www.scss.tcd.ie/doug.leith/privacyofdialerandsmsapps.pdf

- Serveurs DNS hardcodés dans certaines ROM android
- Traceurs et publicités

Backdoors

- 2015 Samsung Galaxy Baseband to Android backdoor: https://redmine.replicant.us/projects/replicant/wiki/SamsungGalaxyBackdoor
- https://en.wikipedia.org/wiki/Backdoor_(computing)#List_of_known_backdoors

Exploitation massive de failles

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

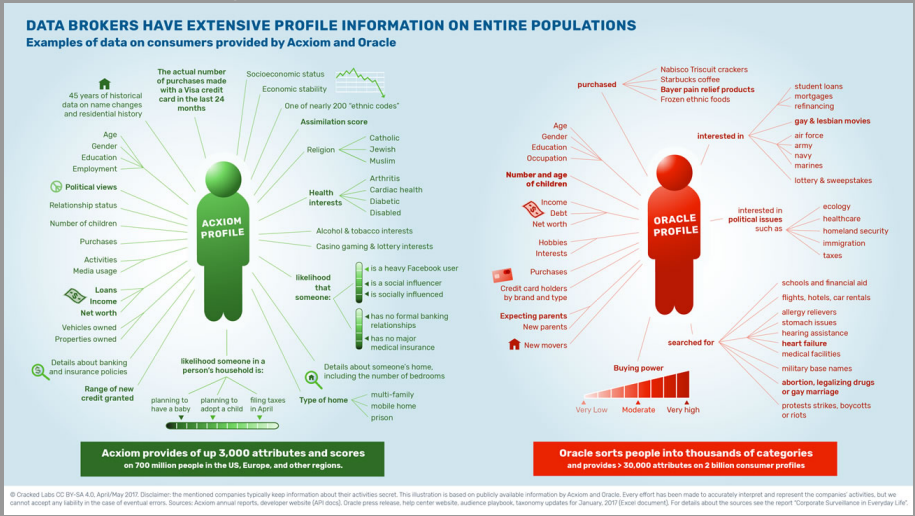
Le problème SS7

- https://eu.rsystems.com/how-can-mobile-operators-secure-their-networks-from-hacker-attacks

Surveillance de masse

- https://www.amnesty.org/fr/latest/news/2023/03/france-intrusive-olympics-surveillance-technologies-could-usher-in-a-dystopian-future/
- https://fr.wikipedia.org/wiki/Surveillance_globale

Oracle, Acxiom, Mixpanel



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

Google WEI

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

Midnight Blizzard

- https://www.theregister.com/2024/04/12/microsoft_cisa_order/

Dépendance

- https://fr.wikipedia.org/wiki/D%C3%A9pendance_au_smartphone
- https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7033082/

Modèle d'addiction et de diffusion malsaine

Tiktok

- https://counterhate.com/wp-content/uploads/2022/12/CCDH-Deadly-by-Design_120922.pdf

Un modèle plus juste ?

- Se passer du numérique
- Agir en connaissance de cause
- Écosystème numérique neutre
- Comprendre et reconnaître
- RGPD ?

Les droits de l'utilisateur

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

Droit à la vie privée

- https://fr.wikipedia.org/wiki/Droit_au_respect_de_la_vie_priv%C3%A9e

Le pouvoir de l'utilisateur d'un matériel informatique, domotique

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 logicielle liée présent sur l'essentiel des appareils prêts à l'usage, il devrait être possible pour l'utilisateur de choisir les programmes qui seront exécutés.

Choix des firmwares

Plus délicat à remplacer que les systèmes d'exploitation, les firmwares sont fournit par les fabricants des composants d'un ordinateur. Ils proviennent d'un ensemble de société d'ingénieurie, R&D développant sous contrat.

Les réseaux

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 ou de communiquer des informations de manière non consentie.

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

Surveillance Étatique

En imposant des rêgles 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 (IETF, IEEE)
- ICANN
- Systèmes autonomes
- Passerelles
- Autorités de régulation (ARCEP en France)
- Opérateurs
- Transitaires

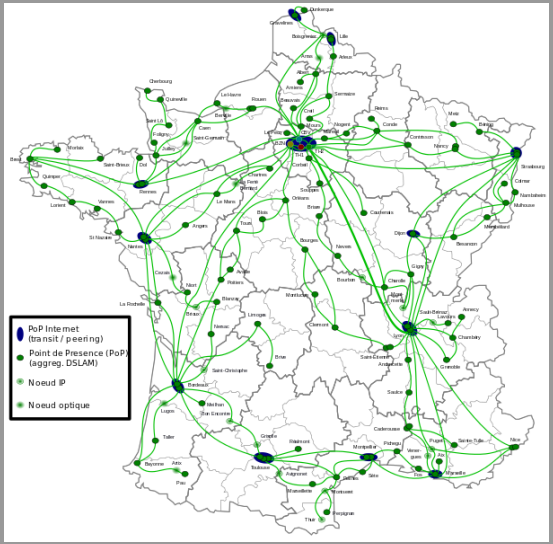


Figure 4: Réseau Free Proxad

- http://jean.godi.free.fr/histoire/fibre.htm

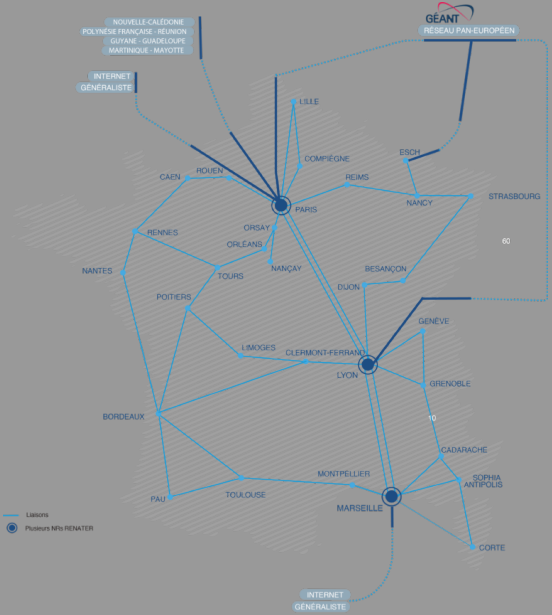


Figure 5: Réseau Renater

- Submarine Cable Map: https://www.submarinecablemap.com/

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, switchs, 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://en.wikipedia.org/wiki/Communication_protocol
- 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.

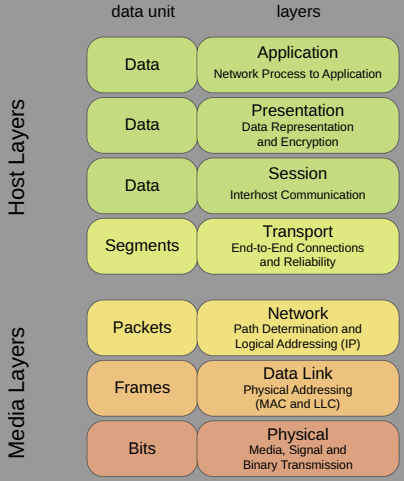


Figure 6: Modèle OSI

IEEE 802

Familles de normes relatives aux réseaux locaux et métropolitains

- https://fr.wikipedia.org/wiki/IEEE_802

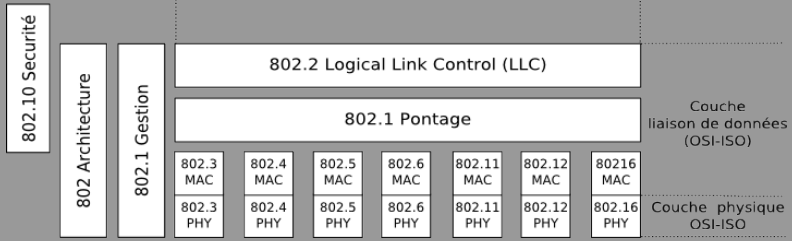


Figure 7: Vue d'ensemble IEEE 802

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
```

IPv4

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
- https://en.wikipedia.org/wiki/Internet_Protocol_version_4

IPv6

L'IPv6 est la version la plus récente du protocole d'addressage d'équipements sur internet, utilisant 128bits au lieu de 32bits en IPv4.

- https://en.wikipedia.org/wiki/IPv6

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.

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 partit de l'écosystème du WorldWide Web il permet 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.

NTP

"Network Time Protocol". Permet la synchronisation des horloges informatiques à l'heure et la date actuelle correcte.

Le modèle client/serveur

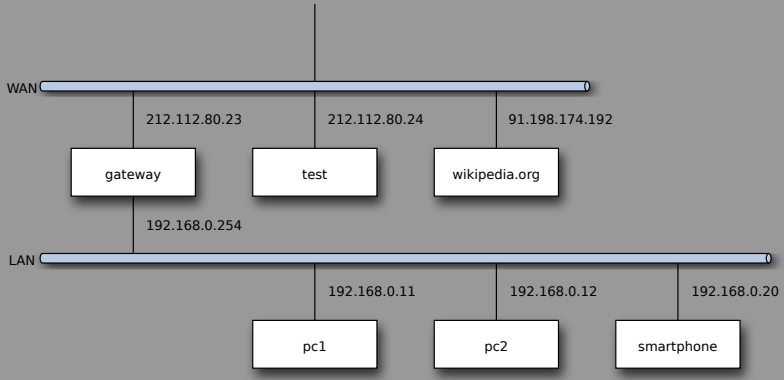
Le “serveur” est un programme donnant accès à des information ou un service. Il attends les requêtes des “clients”. Ces derniers sont les programmes qui parlent un protocole applicatif donné tel que l'HTTP ou le SMTP.

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

Exemple d'une interconnection LAN-WAN typique



Atteintes aux données

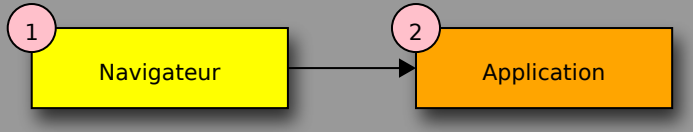
Traçage sur le WEB

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

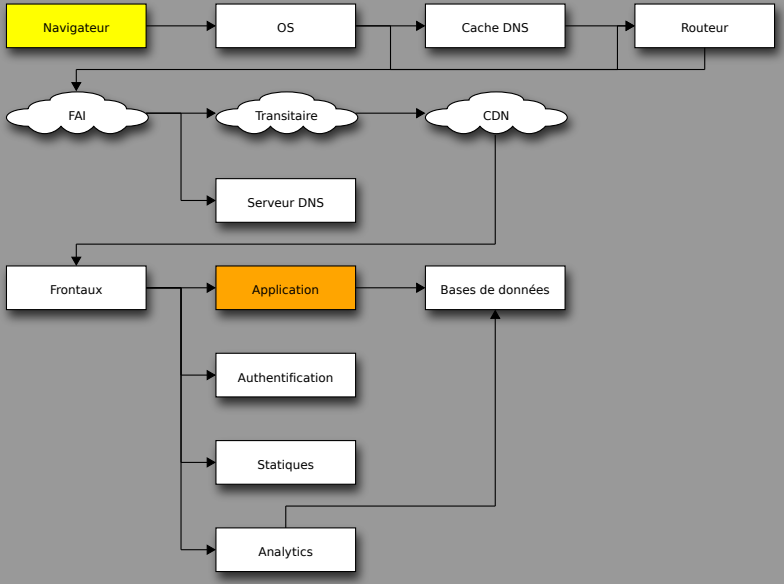
- Caches et CDN
- Load Balancers
- Serveurs HTTP
- Serveurs d'application web
- Bases de données
- Systèmes d'authentification
- Systèmes de monitoring
- Ressources tierces, libs javascript, polices de caractères, publicités

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

Point de vue de l'utilisateur



En pratique


Navigateur
OS
Cache DNS
Routeur
FAI
Transitaire
CDN
Serveur DNS
Frontaux
Application
Bases de données
Authentification
Statiques
Analytics

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.

Que faire en prévention du tracage sur le web

- Considérer d'utiliser le TorBrower ou bien ...

- Utiliser Firefox
- Bien le configurer
- Naviguer sur des sites de confiance
- Utiliser des modules de filtrage
- Opter pour des “Frontend” alternatifs

Quelques modules recommandés

- https://addons.mozilla.org/en-US/firefox/addon/ublock-origin
- https://addons.mozilla.org/en-US/firefox/addon/cookie-autodelete
- https://addons.mozilla.org/en-US/firefox/addon/istilldontcareaboutcookies/
- https://addons.mozilla.org/en-US/firefox/addon/clearurls
- https://addons.mozilla.org/en-US/firefox/addon/libredirect/

Paramétrages

- https://support.mozilla.org/en-US/kb/how-stop-firefox-making-automatic-connections
- https://support.mozilla.org/en-US/kb/firefox-password-manager-alerts-breached-websites
- dom.serviceWorkers.enabled -> false
- javascript.enabled -> false (La plupart des sites seront inutilisables)

Tester les mesures anti-tracage

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

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.

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 sytèmes 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://github.com/emanuele-f/PCAPdroid
- 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 chaine 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

Société

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.

Bugs et failles

Plus un logiciel est grand, plus la probabilité d'y trouver des bugs est grande. L'ajout de nouvelles fonctionnalité 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
- https://www.cert.ssi.gouv.fr/
- https://cert.europa.eu/publications/security-advisories/2024

Systèmes d'exploitation

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

- https://tails.boum.org
- https://www.debian.org
- https://www.gentoo.org
- https://www.openbsd.org

Bootloaders

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

- grub

Principe de moindre privilège

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

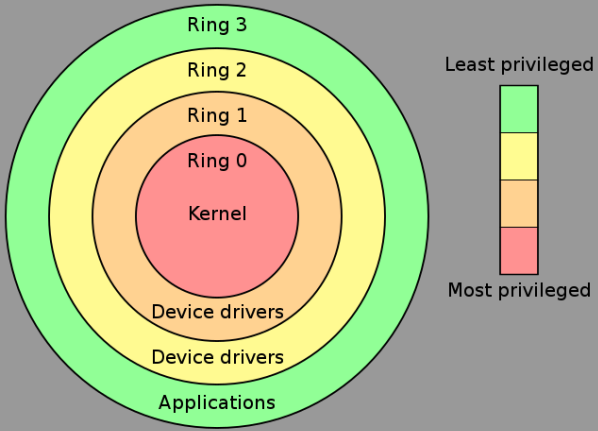


Figure 8: Anneaux de protection x86

Chiffrement des données

Chiffrement matériel

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

Chiffrement logiciel

- https://fr.wikipedia.org/wiki/Argon2
- 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 ressources

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

- Repérer les mails frauduleux
- Ne pas cliquer sur des liens au hasard
- Favoriser des versions de logiciels stables
- Mettre à jour avant d'utiliser
- Utiliser un gestionnaire de mot de passe

On est en 2024

Comment ça sera dans le futur ?