Sécurité numérique et libertés

François Lesueur
francois.lesueur@univ-ubs.fr
@FLesueur / @flesueur@mastodon.social

RAR, Rennes

Université Bretagne Sud, IUT Vannes (Info), IRISA (CASA)

L'objet de cette présentation

Objectif

- Entrouvrir la porte des relations complexes sécurité / liberté / surveillance
- Peut-être aider à comprendre ce malaise / grand écart que certain · es peuvent ressentir ?
- Pourquoi la sécu numérique est ressentie comme émancipatrice / porteuse de liberté alors qu'elle traite de contrôler et limiter les possibilités ?
- Vous donner envie de lire et réfléchir sur le sujet !

Disclaimer

- Je suis certes un scientifique, mais cette présentation n'est pas un travail scientifique
- Je force parfois le trait pour susciter le questionnement, je n'assumerai pas tout !
- Les orgas n'ont pas vu mes slides ;-)

#whoami

Professional side

- Maître de conférences à l'Université Bretagne Sud (Vannes)
- Enseignement et recherche sécurité, réseau, prog
- Développeur de MI-LXC, un simulateur de Mini-Internet

Personal side

- Libriste depuis fort longtemps
- Auto-hébergé et sysadmin du CHATONS KAZ (Morbihan)

Et en tout...

Comprendre et enseigner Internet, sa sécurité, les enjeux

Intro

D'où venons-nous ?

L'imaginaire du hacking : son histoire

- La bidouille. Avant l'Open-Hardware, bidouiller, c'est détourner l'usage / entrer dans la zone grise
- Le *phreaking*. Évader la facturation des appels longue distance. Et la légende raconte qu'ensuite, ils *idlaient*... (et revente, aussi, hein, mais à quelle échelle ?)
- Pirater un jeu, c'est évader les routines de détection parfois très originales déjà !

Ce que cela dit

- Un caractère rebelle, la recherche d'une plus grande liberté quitte à flirter avec l'interdit
- Pas d'impact sur la société (les sociétés de télécoms à la rigueur ;))
- Du petit délit plutôt que de la criminalité organisée

Hacker manifesto, 1986

This is our world now... the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals. Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for. I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all... after all, we're all alike.

LeHack, 2022

Sur les 27 plus gros sponsors, (au moins) :

- 6 entreprises majeures de conseil générique
- 6 étatiques/défense

Mudge 1998 vs Mudge 2022

- Pas de jugement, pas d'orientation
- Mais les choses ont changé, non ?
- La sécurité numérique est-elle un truc de rebelle qui fait rentrer dans le rang ?
- Peut-on être un rebelle à capuche quand on travaille pour le CAC40 / l'armement ?

Ce qui a changé

- Un numérique marginal
- Des attaques peu impactantes
- Une niche plutôt rebelle
- Une contre-culture hacker *underground*

$\Rightarrow$

- Un numérique au cœur de tous les usages
- Des attaques très impactantes
- Une captation par l'organisation historique
- Des hoodies chez les cols blancs

La place du numérique dans la société

La sécurité numérique ne fait que suivre cette place du numérique

La culture

La contre-culture rebelle en friction avec l'intégration au CAC40/banques/armées

La consolidation/centralisation technique

Moxie 1990s vs Moxie 2014

In the 1990s, I was excited about the future, and I dreamed of a world where *everyone* would install GPG. Now I'm still excited about the future, but I dream of a world where / can uninstall it.

Cheminement d'un militant privacy/distribué

- 1990s : PGP vu comme idéal de communication, totalement acentré
- 2011 : Convergence [1] [2], *Trust Agility*, remise en cause de la centralisation des autorités de certification (trop de pouvoir, trop de risque concentré)
- 2014 : Signal, une CA centrale, chemin choisi pour grignoter les systèmes pires

Et ça marche !

Ce n'est pas un hasard

Utilisabilité / Simplicité / Centralisation — Liberté / Distribution

La lutte contre les DDoS volumétriques

Distributed Denial of Service

- L'attaquant se procure des relais de trafic (VPS, botnet, réflection)
- L'ensemble des relais de trafic envoient des paquets vers la cible
- La cible reçoit une avalanche de paquets qui épuisent sa bande passante
- La cible n'est plus capable de recevoir et traiter les demandes légitimes

La protection tierce (Cloudflare, ...)

- En tant que cible potentielle, on fait passer son trafic entrant par un acteur tiers
- Cet acteur a des liens réseau gigantesques, (quasi-)insaturables
- Il est responsable de nettoyer le trafic entrant

$\Rightarrow$ Approche actuelle classique recommandée, centralisation du trafic !

La lutte contre les logiciels malveillants

Le risque et l'historique

- M. Michu télécharge un logiciel sur internet
- Ce logiciel honnête est agrémenté d'un code malveillant (ou le contraire ;))
- M. Michu installe ainsi lui-même, involontairement, ce code malveillant

Les magasins d'application

- Possibilité d'analyser le programme + les retours utilisateurs
- Proactif ou réactif
- De point unique obligatoire (iOS) à point *largement* recommandé (Android)

⇒ Recommandation de sécurité : se limiter au magasin
⇒ Recommandation de liberté : *ne pas* se limiter au magasin

Securité du boot

Le risque et l'historique

- Evil Maid : altération de la chaîne de boot par accès physique (hôtel, douanes, ...)
- Implant suffisamment bas pour être indétectable par les anti-virus

SecureBoot

- Signature et validation dès la sortie de l'UEFI
- Le noyau puis les programmes d'init ne peuvent plus être "quelconques"

Mais qui valide ?

- Des clés racines posées par les constructeurs de cartes-mères
- Dépendance à Microsoft pour signer l'early-boot des OS libres...

(débrayable sur x86, forcé sur ARM)

La consolidation organisationnelle

Le monde a changé

Le numérique au centre de nos organisations

- 1990s : Une attaque n'a pas d'effets à grande échelle
- 2020 : Une attaque peut avoir des effets dévastateurs à grande échelle

⇒ La sécurité de ce numérique, déjà central, devient un sujet (et on s'en félicite)

Comment gère-t-on un sujet ?

- Nous avons une organisation, un modèle économique, un type de société
- C'est cette organisation qui se met en ordre de bataille !

Comment est géré ce sujet ?

- Modèle dominant est le capitalisme, donc *follow the money*
- La sécurité se sculpte sur les rapports de force pré-existants

Exemple d'acteur

L'objectif global de <votre GAFA/BATX préféré> ?

- Un monde meilleur ?
- Un internet au service de tous ?
- D€S PROFIT$?

Sa sécurité

- Une sécurité qui permet de toujours *mieux*/plus commercer en ligne
- *mieux* = moins de risque, plus de responsabilité établissable

Ce que ne sont pas ses objectifs

- Laisser libre choix à l'utilisateur : augmentation du risque
- Garantir la liberté d'expression : pas son périmètre

Exemple d'acteur

L'objectif global de <votre état préféré> ?

- Un monde meilleur ?
- Un internet au service de tous ?
- D€S PROFIT$?

Sa sécurité

- Une sécurité qui rassure ses citoyens *et soit compatible avec le système économique*
- Un besoin de souveraineté sur les décisions (depuis longtemps pour US/Chine)

```
;; ANSWER SECTION:
www.elysee.fr.          3587    IN      CNAME   www.elysee.fr.cdn.cloudflare.net.
www.elysee.fr.cdn.cloudflare.net. 287 IN A      104.18.31.248
www.elysee.fr.cdn.cloudflare.net. 287 IN A      104.18.30.248
```

Concrètement

Qui a le pouvoir sur Internet ?

- Nos états ?
- Des entreprises ?

Qui a le pouvoir sur nos outils numériques ?

- Nos états ?
- Des entreprises ?

Quels investissements dirigent la sécu numérique ?

1. Les grandes entreprises (incluant les entreprises de consultants prestataires)
2. La défense
3. L'état (hors défense), avec des postures contradictoires (protection / surveillance)

Conclusion

Côté société

Sécurité (hors numérique) et liberté

- Pas de liberté sans une certaine sécurité
- Pas de liberté avec une certaine sécurité

Numérique et société

- Plus de société sans numérique
- Plus de numérique sans sécurité

Et donc...

- Notre façon de sécuriser le numérique impacte nos libertés de demain
- La culture du "toujours plus de log", nécessaire pour la sécu/l'audit, n'est pas neutre
- Évident que notre structure de société impacte notre façon de faire de la sécu !

Côté boulot

Sur le marché de l'emploi

- La sécu n'a jamais autant recruté, youpi !
- Mais la sécu qui recrute est évidemment du côté de l'argent...

Interrogation personnelle

- Dans les 1990s, à l'époque de la sécu rebelle, il y avait peu d'emplois ad hoc
- Finalement, aujourd'hui, ce n'est pas pire, c'est juste masqué par la sécu *raisonnable*

Ceux qui font de la sécu aujourd'hui sont-ils ceux qui en auraient fait hier ?

So...

- Des dévs prennent conscience de leur pouvoir et impact (exemple OnEstLaTech)
- La sécu d'aujourd'hui défend *surtout certains* types d'infras, d'une *certaine* façon
- En tant que maillon, important de trouver la structure qui produit du sens ?

Qu'est-ce qu'on fait ? (UPSILON, avec Pablo Rauzy !)

On commence par nommer les choses

- Le vocabulaire, ça offre un espace de réflexion et d'échange
- On acte qu'il y a plusieurs objets à la sécurité

Sécurité asservissante

- Une sécurité qui augmente la dépendance à quelques tiers (oligopole), qui limite la liberté d'action
- Les exemples de cette présentation (centralisation, observation, ...)

Sécurité émancipatrice

- Une sécurité qui augmente le pouvoir des usagers, qui élargit leur liberté d'action
- Accepter que ça implique une plus grande complexité (décentralisation, moins d'observation, ...)

Si vous êtes curieux du sujet

- Hackers: the Internet's immune system, Keren Elazari, TED2014 [Link]
- Why privacy matters, Glenn Greenwald, TED2014 [Link]
- How the NSA betrayed the world's trust – time to act, Mikko Hypponen, TEDxBrussels [Link]
- Ethics in cyberwar times, Ivan Kwiatkowski/@JusticeRage, PTS2022 [Link]

Sécurité numérique et libertés

François Lesueur
francois.lesueur@univ-ubs.fr
@FLesueur / @flesueur@mastodon.social

RAR, Rennes

Université Bretagne Sud, IUT Vannes (Info), IRISA (CASA)