Des records de vulnérabilité

L'insécurité des systèmes informatiques

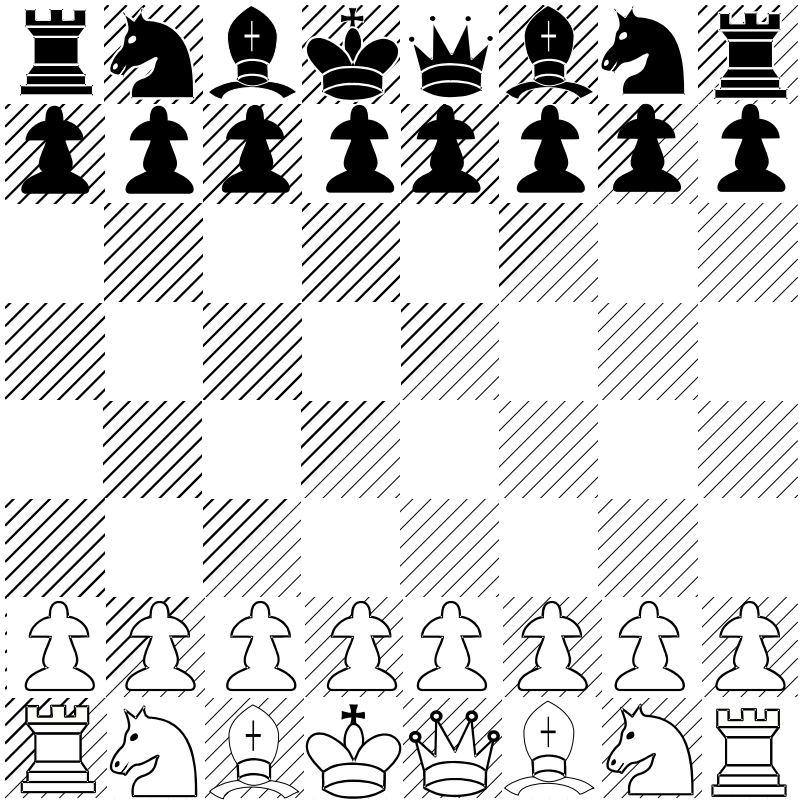
Rodolphe Ortalo

Plan

- Quelques mots sur la « *security* »
- Quel record ?
- Mon idée sur les causes
  - Avec des exemples choisis
- Et puis ce que j'aimerais voir à la place

Des hypothèses de faute bien particulières

- Malveillances
  - humaines
  - intentionnelles
  - avec volonté de nuire
    - directe
    - ou pas
  - et machiavélisme
    - désinformation
    - déguisement



« Lies, Damn Lies and Statistics »

- Attention aux chiffres (et pas seulement...)
- Surtout en sécurité informatique
  - 80% des attaquants sont en interne (ou en externe?)
  - 100% des virus sont des programmes
  - Le piratage coûte des milliards (en 1988, en 2000, en 2014, en 2022 aussi sans doute)
- Vérifiez donc *vous-même*
  - et approfondissez

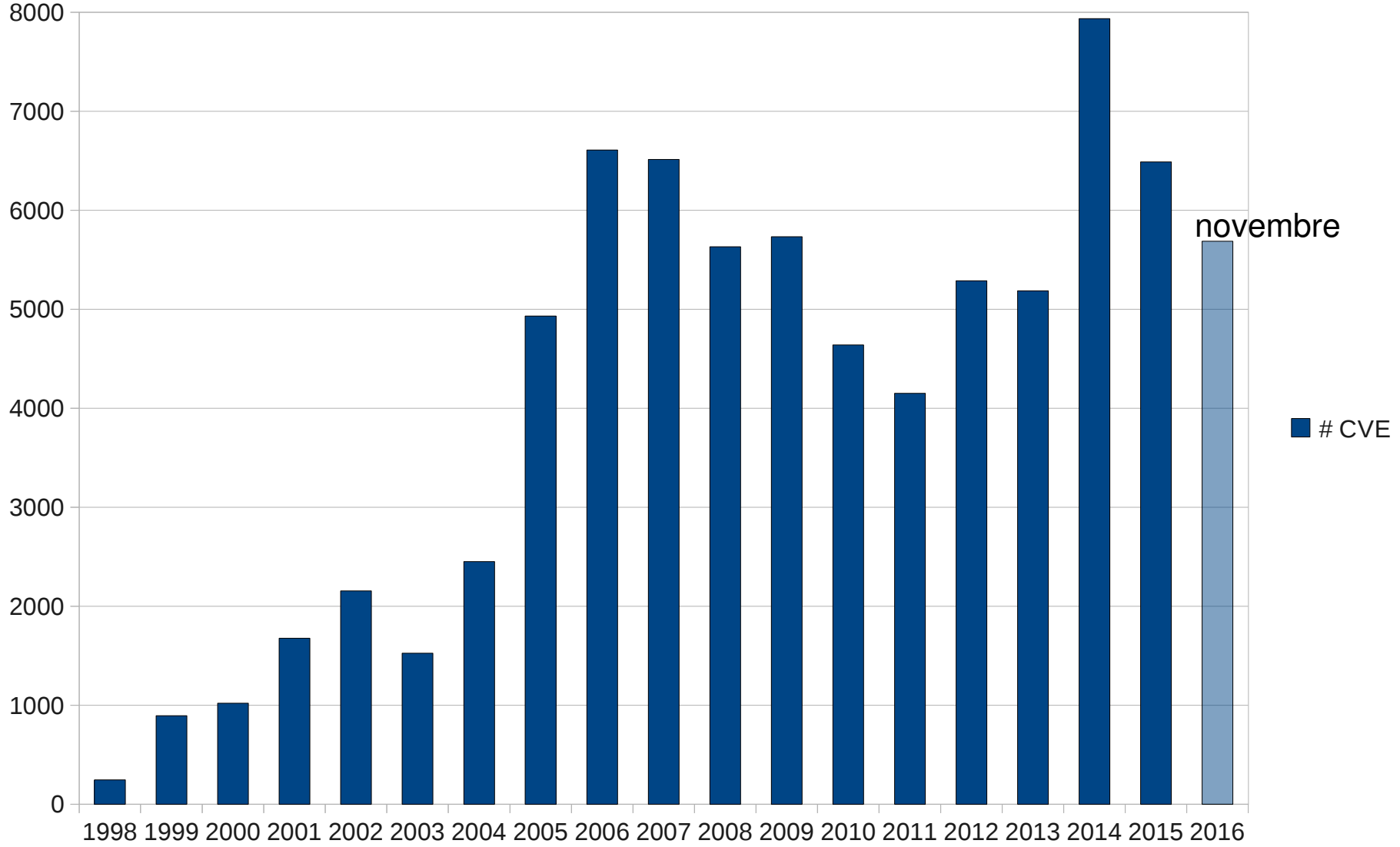
L'origine de cette présentation : l'évolution de la base CVE du MITRE

C'est quoi ?

cve.mitre.org

- The MITRE Corporation
- CVE : Common Vulnerability Exposure
  - Le standard pour la nomenclature des vulnérabilités
  - CVE-*YYYY-NNNN*, par ex. : CVE-2010-2772
- Les CERT, etc.
  - www.cert.org, www.certa.ssi.gouv.fr
  - https://web.nvd.nist.gov/view/vuln/statistics

Des records de vulnérabilité



Source: CVE & NVD

Comment arrive t'on à battre ces records ?

(Là, je commence à devenir désagréable.)

L'essentiel des efforts porte sur l'attaque ou sur des intérêts particuliers

Badass who?

Les intérêts particuliers dominent

- Ceux des pirates
  - L'ego
  - L'argent
- Des communicants
  - Faire de la publicité ou du buzz
  - Journalistes, experts, industriels, etc.
- Des dirigeants
  - Limiter la responsabilité juridique
  - Masquer des risques
- Des acteurs spécialisés
  - agences, industrie, écoles, recherche
    - Obtenir des budgets institutionnels
    - Créer un marché
- Des sociétés commerciales
  - Microsoft, Oracle, Cisco, Airbus, Huawei, Samsung, ...
    - Défendre l'image de marque
    - Protéger le *business*

Pour la protection, les budgets s'évanouissent et les efforts sont fournis chichement

Le développment

Les efforts aussi sont limités

- Les développeurs n'appliquent les règles de programmation qu'à l'école quand ils sont notés
- On trouve peu de volontaires pour auditer du code

- La définition des besoins est toujours sous-évaluée...
  - « On n'a rien a protéger »
  - « On a mis un mot de passe »… pour quoi faire ?

- Ce n'est pas (seulement) une question d'argent
  - Quoi qu'il y ait surtout du boulot pour les débutants
    - C'est une bonne nouvelle pour les débutants...

Les garants se détournent de leur rôle

L'industrie (informatique)

- Vous laisse généralement tomber en cas d'attaque
  - Relisez vos licences et contrats...

    « … *excludes all implied warranties and conditions, including … as much as your local law allows. ... »*
  - Qui a parlé de professionnalisme ?

- Donne la priorité à la défense de son image plutôt qu'à la sécurité de ses clients
  - Certainement des exceptions
  - Ceux qui le disent ne sont pas les pires

Les états

- « Sont les garants de la sécurité des citoyens »
- Les agences ou les services de l'état
  - ont, aujourd'hui, besoin qu'on se rende utile

La loi

- Punit
  - L'utilisation abusive du chiffrement (1939)
  - La constitution abusive de fichiers d'individus (1978 modif. 2004)
  - La copie illicite de logiciels et l'atteinte au droit d'auteur (1988)
  - Les intrusions dans les systèmes informatiques et les vols de données (1988)
    - Y compris en associations (terror.!)
  - L'atteinte à la propriété intellectuelle (1996)
- Créé
  - La base des transactions électroniques (2003)

La loi

- A ma connaissance, continue d'ignorer
  - tout droit à un niveau de protection correct des utilisateurs
    - des garanties de sécurité (soyez pro. !)
  - ou à la connaissance des vulnérabilités
    - possibilité de les rechercher
    - obligation de les communiquer et de les résoudre

- Quid du vice caché ou de la tromperie en matière de logiciel ?

Les autorités de certification

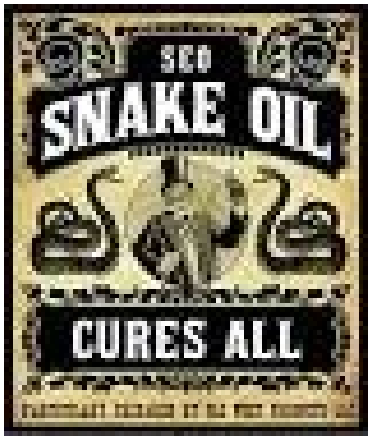
- X.509 et compagnie (les certificats)
  - SSL/TLS, HTTPS, etc.
    - La sécurité du Web quoi...
  - Font l'économie des vérifications de routine
  - Délivrent de vrais/faux certificats
  - Sont compromises dans le plus grand secret
    - Comodo, DigiNotar, etc.
    - Disparition ou *business as usual*
  - On ne sait toujours pas faire de révocation
    - On diffuse des listes noires **dans les navigateurs**
      (Le garant c'est donc le distributeur du navigateur...)

Il vous reste la police ...

- OCLCTIC
  - Si !

- Notez que eux (et les services de justice) sont aussi très inquiets, de...
  - se heurter à d'éventuelles protections informatiques
    - Chiffrement
    - Destruction des preuves
    - Stockage hors d'atteinte
  - Faut-il les rassurer ?
    - Ou leur demander si leurs propres systèmes aussi battent les records ?

La plupart des propositions d'action semblent parfois coupées des réalités



L'avis de l'expert

- Deux grandes options
  - « C'est trop compliqué. On peut pas faire autrement. »
  - « Il ne faut plus utiliser de navigateurs Web avec Javascript, de suite bureautique avec macros, de smartphones et de clef USB. »

Et si on reparlait des compétences des experts?

Petite *checklist* pour les experts

- Transparence et honneteté
- Une formation initiale (un diplôme)
  - Les autodidactes, c'est très rare en fait
- Un socle simple sur :
  - crypto. *et* compilation *et* réseau *et* modèles de sécurité

NB : **Non**, il n'y a pas l'utilisation de `nmap` ou la lecture de MISC

Les mots de passe

- Avec
  - des majuscules, des minuscules ?
  - des chiffres ?
  - des signes cabalistiques (#,-,!$&) ?
- Non !
- Utilisez la puissance de *l'exponentielle*

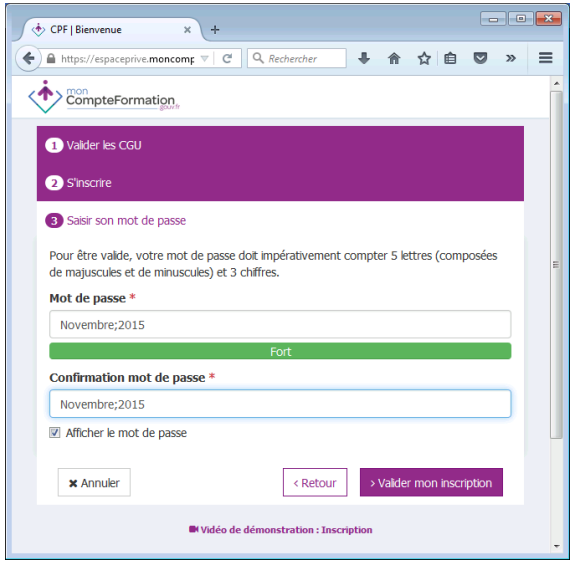
$$26^n$$

Des mots de passe longs !

A la conquête des prix littéraires

- Le *meilleur* mot de passe
  « `Novembre2016!` »

- Un *mauvais* mot de passe
  « `eonpetelq` »



- Racine, Corneille, Shakespeare ?
  - Être ou ne pas être, telle est la question.
  - À vaincre sans péril, on triomphe sans gloire.
  - Ainsi que la vertu, le crime a ses degrés ;
    Et jamais on n'a vu la timide innocence
    Passer subitement à l'extrême licence.

Plus de recettes

- Les correctifs de sécurité
- Les *firewalls*
- Les compartiments et les autres *walls*
- L'antivirus
- Le chiffrement systématique
- L'analyse des risques

Les utilisateurs sont résignés, voire satisfaits

Vous deviendrez j'espère une exception.

Les utilisateurs

- Ca marche ?
- C'est cher ?
- C'est trop compliqué ?
- Je peux télécharger avec ?
- Qu'est ce que je risque ?
- Pourquoi y a pas de licences à accepter ?
- Pourquoi le téléphone ne marche plus ?

La messagerie en ligne

- « C'est facile »
- « C'est gratuit »
- « On y a accès de partout »
- « On peut en changer comme on veut »
- Les conditions d'utilisations : « Oui, j'accepte »

  et
- On a de la publicité bien ciblée
- Les archives sont disponibles
- Et c'est le moyen clef pour contrôler tous les autres authentifiants

Beaucoup de domaines techniques émergents reproduisent fidèlement les erreurs déjà commises

Concrètement

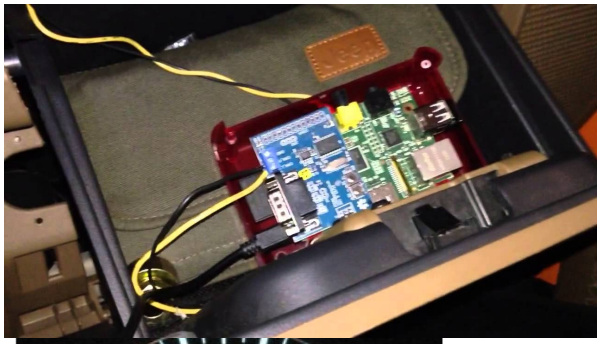


Photo: *resp.*

Security update : Drone firmware

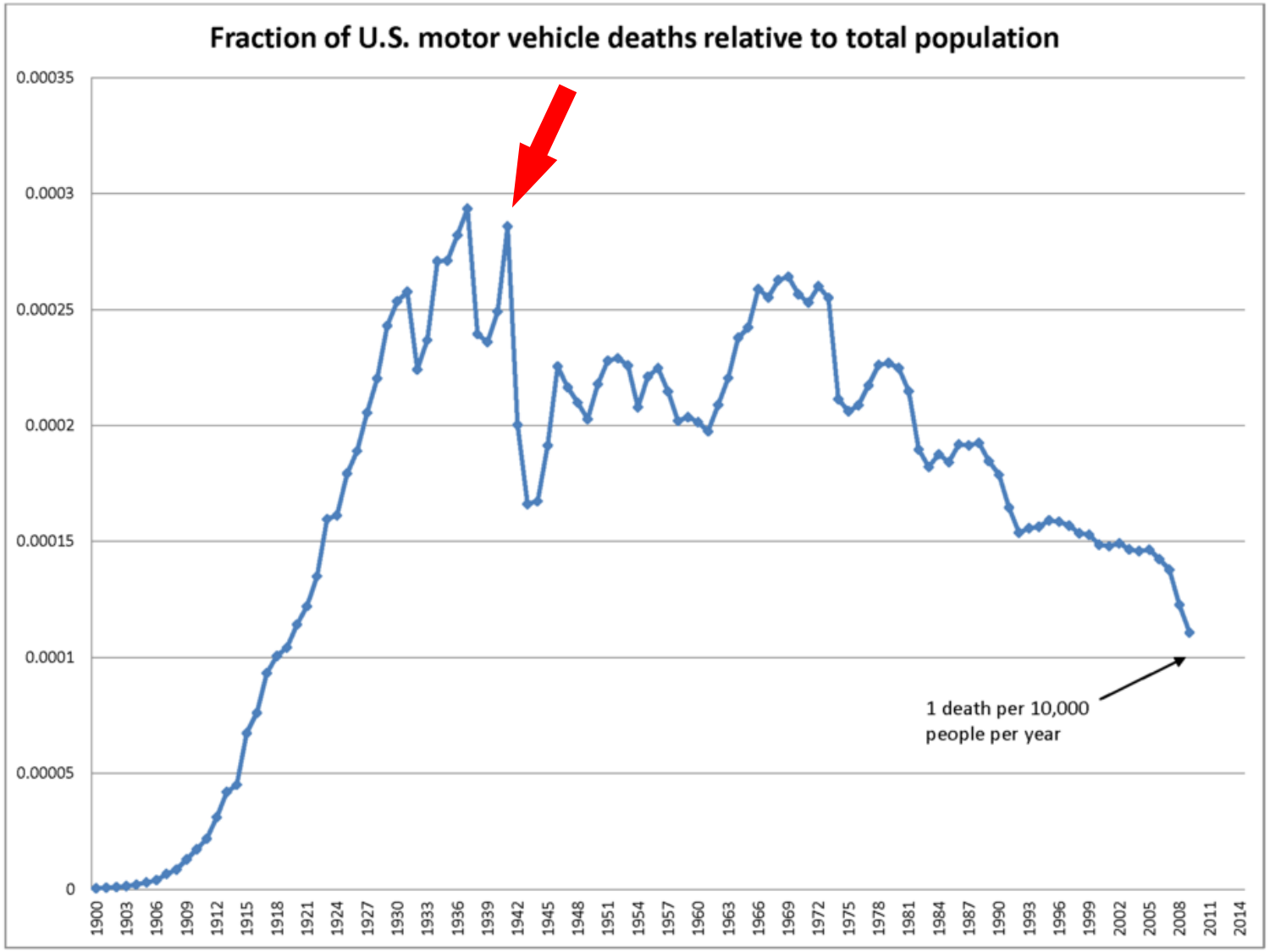
- DJI firmware update
  - february 2015
  - Phantom 2
  - Phantom 2 Vision (+)
- integrates
  - a no-fly zone
  - 15.5 miles radius
  - around the...
    - White House
- et l'Elysée au fait ?

Robot wars

vs.

Derniers détails

- Les plus « vieux » bugs de sécurité identifiés ont persisté jusqu'à 20 ans avant d'être découverts
- L'enregistrement de toutes les données personnelles se généralise, hors des cadres contrôlés
- Kerberos (1988) reste le seul mécanisme distribué déployé largement (mal apparemment, cf. mimikatz)
- On n'arrive toujours pas à lutter contre le spam
- Le nombre de chartes de sécurité aussi bat des records (mots de passe, certification, vie privée, etc.)
  - Et des records d'absurdité



https://en.wikipedia.org/wiki/List_of_motor_vehicle_deaths_in_U.S._by_year via Giant bags of mostly water, Konstantin Ryabitsev, Linux Security Summit 2015.

Alors pourquoi vouloir toujours en faire?

Pour quoi faire de la sécurité?

- Avoir confiance
- Gérer un très grand nombre d'utilisateurs
- Offrir de nouvelles caractéristiques
  - Intégrité
  - Transparence
  - Non-répudiation
- Pair à pair *ou* centralisé

Et comment ?

- Authentification
- Autorisation
- Protocole sécurisés
  - Systèmes distribués
- Modèles de sécurité
  - Intégrés

Et comment donc ?

- Les outils cryptographiques
  - Chiffres symétriques, à clef publique, fonctions de hachage, tatouage, schémas à seuils, SRNG, etc.
- Le développement sécurisé
  - Analyse statique, dév. formel, programmation défensive, compilateurs, etc.
- Les protocoles distribués sécurisés
  - et leur vérification
- sans parler...
  - des protections matérielles
  - de l'IHM de ces fonctions
  - et de tout ce qu'il reste à inventer...

De quoi réver ?

- Pas de mise à jour système pendant 5 ans
- Avoir tous ses contrats signés disponibles
- Ne pas avoir besoin d'une banque pour faire ses transactions financières
- Piloter 50 intervenants qu'on ne connait pas
- Consommateurs et producteurs partageant un même ERP
- Annuler une transaction distribuée
- Créer un état civil mondial (tout de suite)
- Avoir accès aux bulletins scolaires du patron

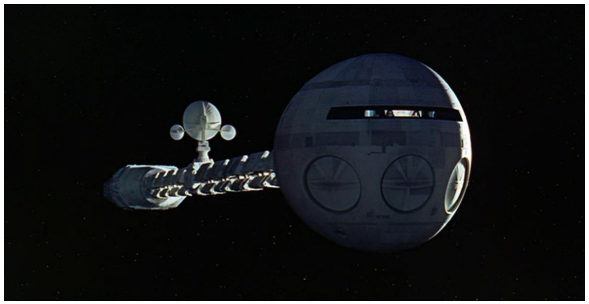
Et le logiciel libre dans tout ça ?

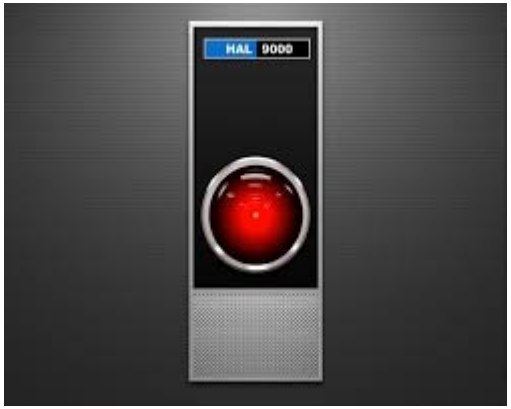
- La conclusion coule de source
  - Elle découle d'ailleurs de la possibilité d'accès au code source

*Comment peut-on avoir confiance dans un logiciel si on n'a **pas** la possibilité de le compiler soi-même ?*

Reflections on Trusting Trust, Ken Thompson, Turing Award Lecture, 1984.

La source du problème





HAL 9000

2001 L'odyssée de l'espace, Stanley Kubrick & Arthur Clarke, 1968.

Note (2010): Contrary to duty imperative, R. Chisholm, 1963.