



# CODI IV

## 4<sup>th</sup> Meeting of the Committee on Development Information « *FOSS and Security* »

### « *Logiciels Libres et Sécurité* »

*E. Bouillon*

*C. Blancher*



- **Etudier en quoi les LL apportent une réponse pertinente aux questions liées à la problématique de la sécurité des systèmes d'information**
  - la problématique de la confiance
  - l'indépendance technologique
- **Illustrations**
  - logiciel libre et transparence
  - standards ouverts et indépendance
- **Conclusions**



- **Caractérisé par sa licence d'utilisation**

- institue un régime de propriété collective qui fournit à chacun :

- ➡ La liberté d'exécuter le programme, pour tous les usages (L 0).

- ➡ La liberté d'étudier le fonctionnement du programme, et de l'adapter à vos besoins (L 1). Pour ceci l'accès au code source est une condition requise.

- ➡ La liberté de redistribuer des copies, donc d'aider votre voisin, (L 2).

- ➡ La liberté d'améliorer le programme et de publier vos améliorations, pour en faire profiter toute la communauté (L 3). Pour ceci l'accès au code source est une condition requise.

- **En quoi ces libertés favorisent la sécurité des systèmes d'information?**



- **La sécurité d'un système d'information résulte d'un équilibre éclairé entre :**
  - le risque associé au SI qu'on protège (C1)
  - le coût des protections mises en œuvre (C2)
    - ☞ impact sur le convivialité d'utilisation
    - ☞ sur la productivité des utilisateurs
  - la pertinence des solutions déployées (C3) par rapport à vos besoins
- **Evaluer la sécurité revient à évaluer la confiance que l'on peut déposer dans un système d'information**
  - que ce soit le sien ou pas.



- **Comment rétablir la confiance dans les composants de son système d'information?**
- **La confiance dans le SI en général suppose la confiance en ces briques de base**
  - son matériel
  - ses systèmes d'exploitation
  - ses applications
  - et aussi ses propres utilisateurs, ses propres administrateurs systèmes et réseau
- **Quelle confiance ?**
  - Nous avons deux façons d'avoir de la confiance
    - ☞ Décider arbitrairement qu'on peut faire confiance
    - ☞ Se donner les moyens de vérifier qu'on peut faire confiance
  - Faire de la sécurité, c'est diminuer la confiance arbitraire (subjective) et augmenter la confiance vérifiée (objective).



- **Permet de vérifier objectivement et exhaustivement ce que fait l'application et comment elle le fait (L1).**
  - Permet de répondre de manière péremptoire à la question de la pertinence des solutions déployées, par rapport aux besoins.
  - Permet de vérifier que ce logiciel n'introduit pas de vulnérabilité dans votre système d'information.
    - ☞ qualité du code évaluée par d'autres personnes que celles qui l'ont écrit ou de la même entreprise
    - ☞ la correction des failles est ouverte à tous les utilisateurs et non à quelques développeurs.
    - ☞ Dans le domaine de la sécurité, l'usage démontre le dynamisme et la réactivité de la communauté des développeurs des logiciels libres.



- **La liberté de modifier le logiciel permet de l'adapter au plus prêt de votre politique de sécurité (L1)**
  - que vous seules êtes à même de définir.
- **La liberté de rajouter des fonctionnalités de sécurité (L3) vous permet d'adapter la solution à vos propres exigences**
  - en cohérences avec le risque que vous aurez estimé.
- **La liberté**
  - d'exécuter (L0),
  - d'adapter(L1)
  - et de faire évoluer (L3),
  - de redistribuer (L2)
    - 👉 vous garantit la **pérennité** de la solution.
    - ✓ respect des normes et des standards ouverts



- **En résumé, le logiciel libre permet**

- **A quiconque**

- **de valider**

- ➡ sa qualité,

- ➡ sa pertinence,

- ➡ sa pérennité

- **Ces vérifications**

- ➡ diminuent la nécessité de confiance subjective

- ➡ tout en créant de la confiance objective

**CQFD**



## ● Dépendance

### ■ La dépendance impose des interlocuteurs incontournables

- ✎ Éditeurs de logiciels choisis
- ✎ Revendeurs agréés par les éditeurs
- ✎ Fournisseurs de services agréés par les éditeurs
- ✎ Mainteneurs agréés par les éditeurs

### ■ Changer d'interlocuteur est

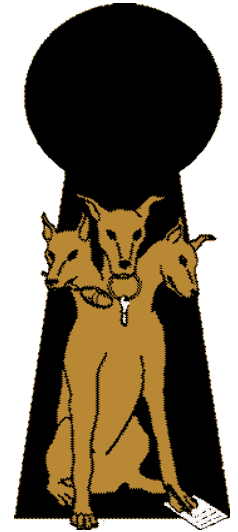
- ✎ difficile (retrouver une société agréés)
- ✎ cher (si on change d'éditeur)
- ✎ peut nuire à la pertinence des solutions en limitant votre choix
  - ✓ ex: service d'authentification avec une base d'utilisateurs stockée dans un format propriétaire, algorithme de chiffrement non standards, ...



- **Les logiciels libres sont indépendants**
  - leur code appartient à tous
- **Indépendance vis-à-vis de l'éditeur**
  - Correctifs de sécurité (L1+L3)
  - Ajout de fonctionnalités (L1+L3)
  - L'évolutivité (L1+L3)
  - Liberté d'expression
- **Indépendance vis-à-vis de la disparition du produit ou de l'éditeur**
  - NT4 n'est plus maintenu, W2000 est en fin de vie
- **Indépendance vis-à-vis du fournisseur :**
  - Disponibilité (L2)
  - Maintenance (L1+L3)
  - Déploiement (L0)
  - Support (L1+L2+L3)
- Application nationale (e-gouvernance) : logiciel libre et souveraineté (B. Kagai FOSSFA)



- **Kerberos est un protocole d'authentification réseau**
  - standard (RFC 1510)
- **Il existe plusieurs implémentations**
  - Propriétaires
    - ☞ AD (Microsoft), SEAM (Sun Microsystem)
  - 3 open source dont 2 (MIT, Heimdal) sont
    - ☞ Parfaitement opérationnelles
      - ✓ Employées en production sur de grands sites
    - ☞ Font référence vis-à-vis des implémentations propriétaires (AD, SEAM, ...)
    - ☞ Sont meilleures
      - ✓ en fonctionnalité
      - ✓ Souplesse / adaptabilité
      - ✓ Stabilité
      - ✓ Portabilité (!)
  - Des expériences malheureuses ont été rencontrées lors de choix « propriétaires »





- **Forum de discussion dédié à Kerberos**

- MIT vs Heimdal?

- ✎ Les développeurs du MIT et de heimdal participent à la discussion

- ✎ Expliquent dans quelles conditions techniques telle ou telle implémentation est préférables

- Quelles sont les chances d'obtenir le même débat

- ✎ facilement

- ✎ publiquement

- ✎ en toute objectivité technique

- ✎ entre un développeur de SEAM et de AD ?



- **Authentification forte ou « 2 facteurs » :**
  - ex :
    - ☞ l'utilisateur doit connaître un secret (mot de passe, code PIN)
    - ☞ ET posséder un objet (carte à puce, crypto-processeur USB)
- **Certains de ces matériels fonctionnent selon des standards**
  - PKCS #15, PKCS #11
- **Pour ces matériels, les développements utilisant l'API standardisée sont toujours utilisables même si on change de fournisseur**

## « Information en tant que ressource économique »

- **Cette affirmation reconnaît l'impérative nécessité de protéger cette information.**
  - la sécurité est un service essentiel du système d'information
- **Une mise en péril de la sécurité du système d'information provoque**
  - une perte directe
  - un discrédit
- **La sécurité**
  - n'est pas quelque chose que l'on achète,
  - ni un état,
  - mais un processus.

## « Information en tant que ressource économique »

### ● Le risque :

- une caractéristique essentielle de l'information est qu'elle ne perd pas de valeur dans son transport
  - ☞ pas de perte en ligne comme pour l'électricité
  - ☞ permet de s'affranchir a priori des contraintes géographiques
  - ☞ revers : l'agresseur potentiel est partout, sa portée est mondiale
- en 2001, l'espérance de vie d'une RedHat 6.1 non à jour connectée à Internet était de quelques heures
- impunité

## « Information en tant que ressource économique »

- **La valeur de cette ressource n'a de sens qu'en rapport avec la sécurité qui lui est associée**
  - Les axes de cette sécurité
    - ☞ confidentialité (authentification, autorisation, ...)
    - ☞ intégrité
    - ☞ disponibilité
  - Pour chacun de ces points, les LL offrent des solutions techniquement pertinentes

- **Pour alimenter votre réflexion:**

- **Projet Tera-10 du CEA**

- ☞ en 2001, Tera-1 (5 Teraflops)

- ☞ en 2005, Tera-10 (60 Teraflops)

- ✓ 4532 processeurs,

- ✓ 27 000 Go de mémoire,

- ✓ Interconnexion de 100 Go/s,

- ✓ un milliard d'octets d'espace disque.

- ✓ Système d'exploitation : ***GNU/Linux***

- ✓ Système de fichier parallèle : ***Lustre (open source)***





- **Cet exposé avait deux objectifs:**
  - Prise de conscience du risque et de la nécessité de considérer la sécurité des systèmes d'information
  - Démontrer la pertinence des logiciels libres dans ce domaine

**Merci de votre attention**