

# TCPA, Palladium, EUCD

*ou Mickey et la Machine Infernale*

Thomas Tempé

`Thomas.Tempe@insa-lyon.fr`

Groupe de Pingouins Libres

# Avertissement

Cette histoire comporte une part de réalité, et  
une part de spéculation.  
Elle est arrivée près de chez vous.

# Les protagonistes

- **Les méchants** : Le *Grand Méchant Loup* (la RIAA Recording Industry Association of America) et les *Petits Mickeys* (Disney)
- **Leurs serviteurs** : Microsoft et IBM
- **Les instruments du mal** : le DRM
- **Le narrateur** : votre serviteur
- **La victime** : vous

# La Machine Infernale

DRM ( **D**igital **R**ight **M**anagement ) :  
Technologie permettant de contrôler la manière  
dont est utilisé un fichier

- Enregistrement musical qu'on ne peut lire que 3 fois
- Bande-annonce de film avec une date d'expiration
- Rapport lisible uniquement sur les ordinateurs de la société X.

# Une Grande Vision

- Endiguer le phénomène *Napster*
- Empêcher l'exécution de logiciels interdits
- La location de logiciels
- La croissance du commerce électronique
- Le contrôle des activités des employés

# Les difficultés

- Les mécanismes anti-piratage ne marchent pas
  - il y a toujours une faille
  - le problème du *crack once run anywhere*
  - on n'a pas le droit d'interdire les utilisations légitimes (copie privée...)

# La solution

Contrôler ce que fait l'utilisateur avec son ordinateur

- Empêcher la conversion d'un fichier audio sécurisé au format .mp3
- Empêcher l'utilisateur d'enregistrer ce qu'il joue sur sa carte son
- Brouiller le signal audio pour empêcher de brancher un enregistreur à la place du haut-parleur...

# La solution

Un grand chantier :

- Protéger l'ordinateur contre l'utilisateur
  - l'application
  - le système d'exploitation
  - la carte mère...
- Crypter tout le contenu, et rendre sa lecture dépendante de serveurs de droit
- Révoquer le droit d'utilisation des programmes qui s'avèrent défectueux...

# La construction de la machine

# Un scénario en trois parties

- Sécuriser le matériel
- Blinder le logiciel
- Adapter la loi

# Le matériel

## Comment sécuriser le matériel ?

- Authentifier de manière sûre chaque ordinateur
  - Clé privée et processeur cryptographique sur la carte mère
  - Numéro d'*activation* de Windows XP
- Certifier que le système d'exploitation est *de confiance*

# Le matériel

- *La Fritz Chip*
  - nommée après le sénateur américain qui veut la rendre obligatoire aux E-U.
- Le TCPA (Trusted Computing Platform Alliance)
  - une architecture standardisée

# Le matériel

Ce qui existe aujourd'hui :

- Les consoles de jeu récentes (X-Box, PS2) ne démarrent que des systèmes d'exploitation signés
  - impossible de changer le système d'exploitation
- Les nouveaux portables IBM Thinkpad intègrent le support T CPA

# Le logiciel

- Un système d'exploitation qui contrôle les applications exécutées
  - offre des services DRM aux applications
  - privilèges pour les applications signées
  - refus éventuel des applications non signées

# Les applications...

- encryptent toutes les données
- les rendent lisibles uniquement à des applications *de confiance*
- empêchent l'interopérabilité, et la modification des droits par un logiciel tiers

# Exemples d'utilisation

- Word DRM pourrait interdire la lecture d'un article jugé subversif
- Un patron pourrait interdire la diffusion de rapports internes hors de l'entreprise
- ...

# Les modes DRM/Sans DRM

- Le contenu DRM est crypté et lisible uniquement en *mode DRM*
- Certains contenus ne seront accessibles que en mode non/DRM

# Les modes DRM/Sans DRM

- Si tout le monde utilise le mode DRM par défaut, on est obligé de l'utiliser aussi
- Difficulté de signer du logiciel libre
- Conflit idéologique : *information wants to be free*

# Le logiciel

- Microsoft a le monopole (par brevet) sur les systèmes d'exploitation intégrant la gestion des droits.
- *Palladium* : sera intégré dans le prochain Windows (*Longhorn*)
- Sony développe sa propre technologie DRM

# Le logiciel

## Ce qui existe aujourd'hui

- Windows Media Player 9 peut télécharger et révoquer des modules de décryptage sécurisés

# Finir comme les amiagistes

- tout le monde pourra désactiver le mode DRM (dans un premier temps, et sauf sur la X-Box, la PS2, l'ordinateur de l'entreprise...)
- le monde pourrait être coupé en 2 :
  - les utilisateurs de DRM
  - les autres

# Le volet légal

- Les lois qui interdisent de contourner les “systèmes de sécurité”
  - Aux États-Unis : DMCA, depuis 3 ans.
  - Directive européenne : l'EUCD
- Les lois qui rendraient obligatoire l'ajout de puces DRM sur tout appareil électronique (télé, magnétoscope, caméra...) : discussions aux États-Unis

# Des lois mal faites

- ne protègent souvent pas les contournements légitimes de systèmes de sécurité
  - lecture de DVD
  - recherche en cryptographie
  - mise à jour de failles de sécurité

# Des lois mal faites

- Protègent des utilisations illégitimes de systèmes
  - le zonage des DVD
  - le cas des cartouches Lexmark
  - Adobe et le E-Book

# L'EUCD

- Loi française en cours de discussion
- Menace sur la copie privée
  - interdiction de copier ses CD pour les lire dans la voiture
- Initiative <http://www.eucd.info>

# Conclusion

## La gestion numérique des droits

- Un avenir incertain
- Ça arrive très vite
- Ça sera installé par défaut sur beaucoup d'ordinateurs
- Une concentration de pouvoir dangereuse

# Mes recommandations

- Utiliser des formats ouverts (OpenOffice.org...)
- Ne pas utiliser Windows XP, ni les fichiers .wma
- En parler autour de soi
- Aller lire <http://www.eucd.info>

# Conclusion

L'histoire de l'informatique est l'histoire d'une longue bagarre entre les constructeurs, qui veulent rendre leurs clients captifs, et les utilisateurs, qui veulent utiliser leur ordinateur malgré tout.

# Redistribution de ce document

Copyright 2003 © Thomas Tempé.

Permission est accordée de distribuer et modifier ce document selon les termes de la licence *GNU Free Documentation Licence* dans sa version 1.1 ou postérieure, telle qu'elle est publiée par la *Free Software Foundation*.

Ce document entrera dans le domaine public au plus tard dix ans après sa création.