

Securité des portables sous Linux (FR)

Author: Werner Heuser - TuxMobil.org

Traduction: Nicolas Barcet – barcet.com

Méthodes de sécurisation du portable Linux contre le
vol et la perte

Werner Heuser (TuxMobil)

<http://tuxmobil.org>

Version 1.0

Statistiques de vols (FR)

- 620.000 portables volés aux USA en 2002 1)
- “.. le coût moyen de la perte d'un portable pour une entreprise est de \$89,000 ..” 2)
- Annonces hebdomadaire dans la presse au sujet de portables volés contenant des données sensibles.

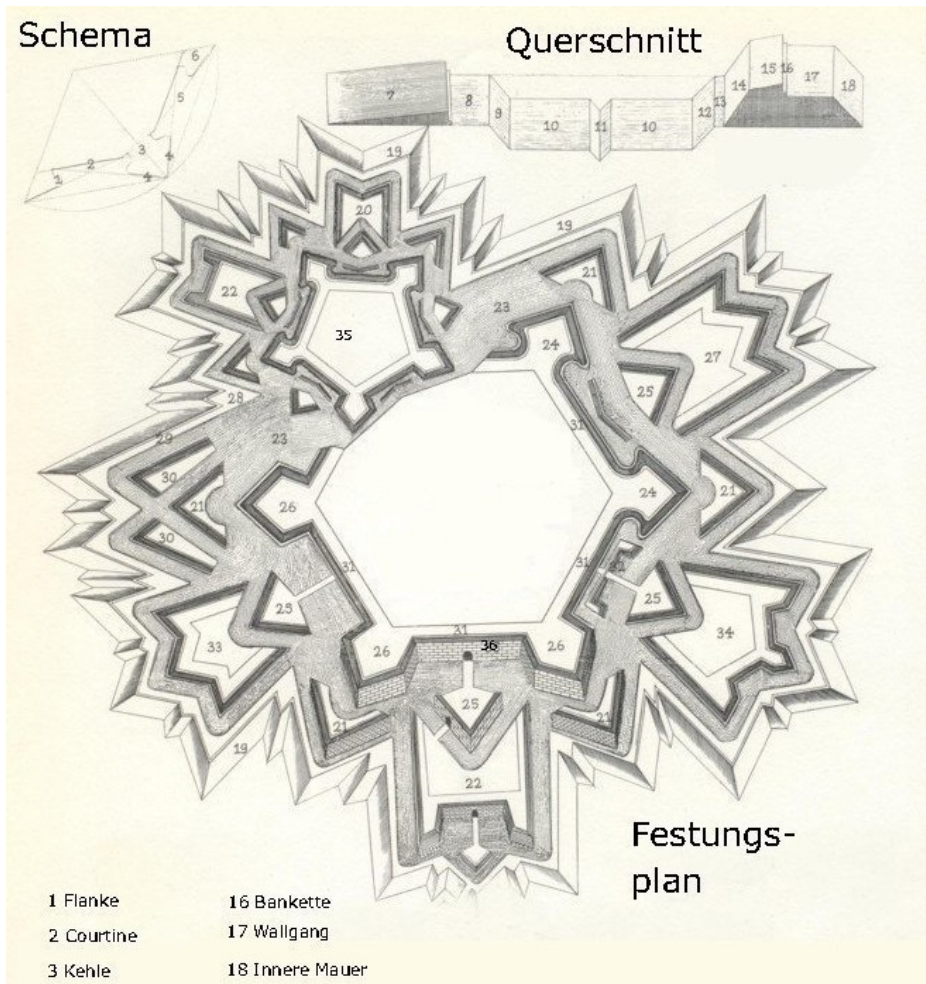
Echèle de risque (FR)

- Perte matérielle : Côté de récupération, temps de travail perdu, reconfiguration
- Vol de données : informations internes confidentielle et données client
- Vol d'identité : mot de passe, profil utilisateur
- Mauvaise pub : impact sur l'image de l'entreprise

Il y a-t-il une solution parfaite ? (FR)

- Pas de 100% contre la perte et le vol
- Bonne protection via :
 - Comportement humain
 - Configuration sécurisé du système
 - Outils de sécurité Hard et Soft

Métaphore de la forteresse (FR): La meilleure sécurité est multiple



- Doutes
- Bassins
- Obstacles mobiles
- Hauts murs
- Canons
- Soufre, plomb...

Securité = Compromis (FR)

“La sécurité n'est jamais parfaite, c'est toujours un compromis.”

-- Bruce Schneier [1\)](#)

Depuis le début :

Achat d'un portable (FR)

- Achat d'un portable neuf :
 - Conserver la facture et le numéro de série en lieu sûr.
 - L'enregistrement chez le constructeur est associé avec une base de données des vols.
- Achat d'un portable d'occasion :
 - Vérifier avant d'acheter (bases de vols).
 - Exiger les manuels originaux et les factures afin de bénéficier de la garantie et pour confirmer l'origine.
 - Scannez la carte d'identité du vendeur

Moyens physiques (FR)

- Cables de verrouillage
- Fixations
- Détection de mouvement (PCMCIA)
- RFID
- Auto-collants
- Gravure
- Vis pour CD/DVD, DD (ThinkPad)

Cable de verrouillage (FR)

- Fente Kensington
- Techniques de contournement
 - Crochetage
 - Force brute :
 - Cisaille
 - Destruction du point d'attache
 - 10.000 combinaisons = 3 heures



Auto-collant (FR)



- Inventaire et protection contre le vol
- Rend la revente difficile
- Peut être enlevée, quoi qu'en dise le fabricant
- Fabricant : stoptheft.com

Vérou sans fil USB (FR)



- L'adaptateur USB verrouille le portable si l'utilisateur s'éloigne de 2m
- Driver linux vp-usb-lock [1\)](#)
- CONRAD.DE
Art.-Nr. 997993 – RV
19,95 Euro

Critique du Véro sans fil USB (EN)

- Peu de documentation (presque rien sur l'interaction avec PAM)
- Driver Linux ne compile pas avec le Kernel 2.6.19
- Driver Linux ne semble pas fonctionner avec un driver souris USB
- Sécurité très relative :
 - Protection par mot de passe seulement
 - Connection sans fil interceptable

Carte PCMCIA Caveo (FR)



- Alarm de détection de mouvement
- Pas de drivers pour Linux
- Pas de réponse du fabricant à de multiples requêtes

Customisation (FR)



- Technique de protection
 - Difficulté de revente
 - Facile à reconnaître
- Problèmes
 - Difficulté de revente
 - Possible à enlever

Sac : Camouflage (FR)



- Pouvez vous deviner ce qu'il y a dans ce sac ?
- Un bon camouflage évite de susciter l'envie

Assurances (FR)

- Société d'assurance dédiés : exemple safeware.com aux USA (vol et dommages)
- Fabricants de portables : certains proposent une garantie étendue incluant le vol

Mot de passe BIOS (FR)

- Non disponible sur tous les portable, généralement sur les marques : ex. Samsung, IBM/Lenovo.
- Les media de restauration de mot de passe doivent être créés sous windows

Encryptage BIOS du Disque Dur (FR)

- Uniquement disponible sur les modèles les plus chers (ex. IBM Thinkpad)
- Media de récupération ne peuvent être créé que sous Windows
- Positif : simple à mettre en oeuvre
- Négatif : certaines sociétés de récupération de données proposent le décryptage

Logo BIOS (FR)



- Non disponible sur tous les bios
- HOWTO pour Linux disponibles (ex: thinkwiki.org)

Customisation (FR)

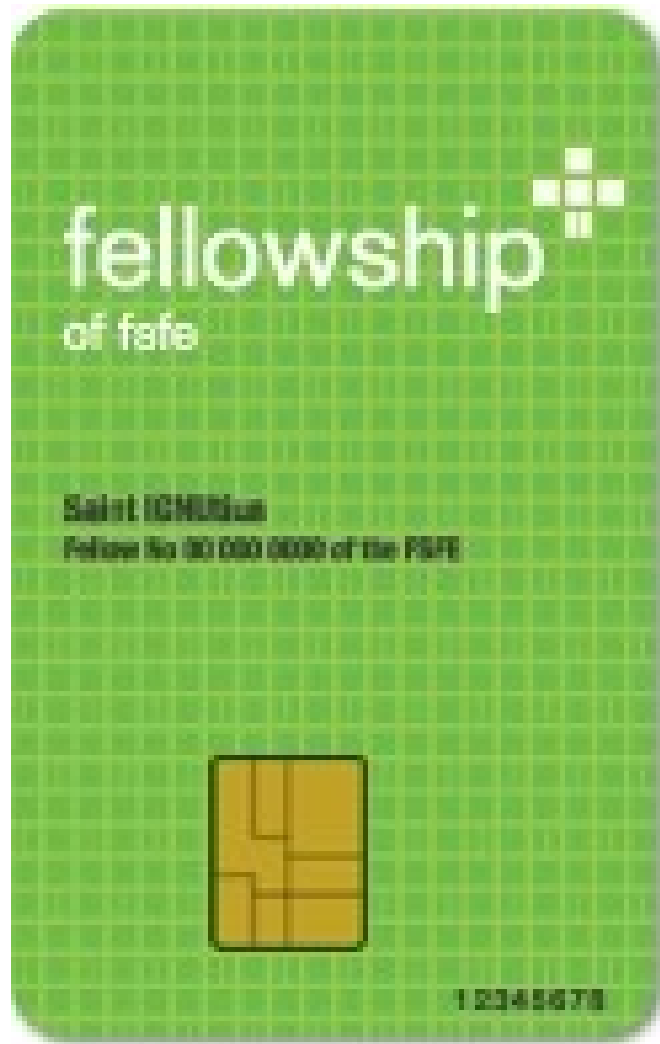


- Technique de protection
 - Difficulté de revente
 - Facile à reconnaître
- Problèmes
 - Difficulté de revente
 - Possible à enlever

Lecteur d'empreintes digitales intégrés (FR)

- Offre une protection limité
- Contournement du lecteur via
 - Linux Live CD (ex: Knoppix)
 - Passage en mode console ou seconde console
 - Vol d'empreintes

Carte à puce (FR)



- avantage: stockage de la clef sur un media externe
- exemple: Carte OpenPGP
 - Encryptage (presque) fonctionnel sans intervention avec le Kernel et GnuPG courant
 - login (PAM) doit être adapté ¹⁾
- autres concepts: [OpenSC](#), etc...

Carte à puce (FR)



- Peu de portable équipés d'un lecteur 1)
- Lecteurs USB externes peu pratiques pour un usage mobile
- PCMCIA : le lecteur OmniKey CardMan 4040 est reconnu sous Linux
- Cartes par **FSFE**, **g10code**

Trusted Platform Module: TPM (FR)

- TPM offre les bases de la confiance pour la mesure CRTM
- Peu de portable avec TPM pour l'instant (qq. ThinkPads)
- Le support de Linux pour TPM n'est pas encore utile pour la sécurité



Sauvegarde (FR)

- Disque Durs externe 2.5" sont pratiques et pas chers
- Clefs USB sont généralement suffisante pour une sauvegarde de \$HOME
- Solutions de bakup et systèmes de fichier pour la synchronisation mobile (AFS, SVK, Coda, ...)

Encryptage (FR)

- Méthodes:
 - DM-Crypt et LUKS
 - TrueCrypt (également disponible pour MS-Windows)
- Recommandation : encrypter au moins \$HOME
- Failles :
 - Zone swap
 - Fichier de mise en veille et partitions
 - /tmp, /etc, /var/log
- Références : Linux-Magazin 10/2006 Seite 33ff.

Outil d'alarme (FR)

- Apple PowerBook/MacBook et IBM/Lenovo ThinkPad incluent un “airbag” pour disque dur (HDAPS).
- HDAPS peut être utilisé comme une alarme
- Alarme déclanchée par un déplacement du portable
- Source: thinkwiki.org

Lecteur d'empreintes USB (FR)



- Zone de stockage externe (\$HOME)
- Quelques modèles fonctionnent avec Linux MAIS ne se configurent qu'avec MS-Windows.
 - iX 10/2006 p. 76
 - <http://www.heise.de/mobil/artikel/79122>

Recommandation: 4 techniques simples (FR)

- Marquage : gravure, auto-collant, bootloader
- BIOS : mot de passe et encryptage
- Encryptage du DD : au moins \$HOME
- Sauvegarde : \$HOME sur clef USB

The End (FR)

Merci et bonne visite de Solutions Linux

Critiques, questions, remerciements :
<wehe@tuxmobil.org>

présentation :

<http://tuxmobil.org/presentations>