



Opération pilote de déploiement d'une solution de protection des portables à l'IN2P3

Chiffrement des disques des portables



Appréciation des risques

- Vulnérabilité : portabilité
- Menace : vol, emprunt
- Impacts : confidentialité, disponibilité, intégrité
- Vraisemblance : élevée
- Risque inacceptable
- Mesure de sécurité : chiffrement

Chiffrement intégral du disque

- Simplicité
 - Authentification au démarrage puis transparent
- Sûr
 - Temporaires, swap, hibernation, registre, système de fichiers journalisé, etc.
- Bonne réponse à la menace de vol et aux conséquences en matière de perte de confidentialité

- Logiciel
 - Bitlocker : Vista Ultimate ou Enterprise
 - Truecrypt : Windows XP ou Vista
 - Dm-crypt + initrd + installation : distributions Linux récentes
- Matériel, disque chiffrant
 - Seagate Momentus 5400 FDE.2
 - Hitachi Travelstar 7K200
 - Prochaine génération chipset Intel (Danbury)

- IN2P3
 - Taille significative
 - Homogénéité
 - Culture de sécurité
 - Structuré
- Nouveaux portables
 - Logique pour un commencement
 - Pas de problèmes pour chiffrer l'existant
 - Taux de renouvellement important
 - Les existants dans un second temps
- Installation, configuration par équipe technique

- Installation initiale
- Recouvrement
- Besoins d'assistance et acceptation
- Sauvegardes
- Maintenance
- Compatibilité avec les applications
- En phase avec les évolutions du marché et les méthodes d'attaque

- Difficultés rencontrées
- Coûts et moyens à mettre en œuvre
- Economies réalisées
 - Conserver un disque en panne
 - Mise au rebut
- Amélioration effective de la sécurité
- Acceptation par les utilisateurs
- Déploiement à l'ensemble du CNRS

- Cold boot attack
 - Persistance de la mémoire
- Pre-boot authentication
 - Jonathan Brossard à Defcon 2008
 - Caractères clavier → tampon BIOS (0x41e)
 - Oubli d'effacer ce tampon avant et après
 - Le mot de passe persiste et est récupérable
 - Bitlocker : vulnérable, corrigé Vista SP1
 - Truecrypt : 5.0 vulnérable, 6.0a non

Conclusion

- Tendance : intégration du chiffrement dans le logiciel ou le matériel
 - Surcoût faible
 - Risque d'utilisation sauvage (absence de recouvrement)
- Réel besoin de chiffrement
- Important de valider l'organisation autour du chiffrement
- Ne dispense pas d'autres mesures de sécurité