1. Présentation de LexBOX

Présentation faite par MM. Jean-Claude Escriva et Jacques Debiez.
Présentation : http://www.ossir.org/resist/supports/cr/20050926/LexBOX.pdf
Guide des scellés informatiques (DCSSI) :
http://www.ssi.gouv.fr/fr/documentation/Guide_scellesV1.0.pdf

« L'ennemi, c'est l'administrateur système ». Usuellement, l'administrateur système dispose de tous les droits sur les fichiers du ou des systèmes qu'il gère. Cela produit de nombreuses difficultés quant à la preuve formelle (juridiquement valide) de l'authenticité des informations qui sont extraites d'un ensemble informatique.

L'objectif de LexSafe est de construire cette « preuve informatique ». Le produit définit le concept d'original d'un document électronique, un original non-falsifiable, non répudiable, dûment horodaté. Il est à noter qu'il existe un vide juridique autour de cette notion d'original électronique, et aucune loi n'aborde la problématique du stockage, de la conservation et de l'archivage des données.

LexSafe est un équipement de stockage de confiance des données. De façon intéressante, il reprend un grand nombre des éléments du Guide 931 des scellés informatiques, diffusé par la DCSSI (voir le document concerné sur le site de la DCSSI : http://www.ssi.gouv.fr/fr/documentation/Guide_scellesV1.0.pdf).

Qu'est-ce qu'une preuve informatique ?

- Un enregistrement : stockage et archivage
- Protégé : intégrité, inaltérabilité (maintien des données dans le temps), gestion des accès et de la confidentialité
- Daté : horodatage non modifiable
- Identifié : sceau unique, auto-généré, de l'équipement.

On se rapproche d'un stockage de type WORM dans les fonctionnalités d'écriture (une fois) et de lecture (autant de fois qu'on veut). Pour éviter les problèmes, les commandes d'accès au support (lecture, écriture, effacement...) sont filtrées avant leur transmission au pilote du disque.

Lors de l'écriture d'une information, celle-ci est datée, en utilisant l'horodateur embarqué de l'équipement. Au besoin (selon la configuration), elle peut être chiffrée, à l'aide d'un sceau spécifique à l'équipement.

Du point de vue de la fabrication, il existe plusieurs couches physiques de protection/scellement de l'équipement, pour empêcher l'extraction du sceau de chiffrement. Des méthodes actives provoquent la destruction du sceau (et donc

l'irrécupérabilité des données) en cas de tentative d'intrusion physique sur l'équipement.

Le scellement chimique du boîtier permet de garantir l'authenticité de l'équipement. S'il un boîtier est présenté comme preuve, LexBOX peut vérifier facilement qu'il s'agit bien du « bon » équipement et que celui-ci n'a pas été bidouillé. La méthode de scellement chimique repose en grande partie sur l'aléa naturel produit par des mélanges dans lesquels des particules sont injectées.

Le boîtier procède à une réécriture régulière des données, avec détection d'éventuelles différences entre l'original et la copie. Ces erreurs venant généralement d'un problème sur le support, le système alerte l'opérateur puisque la « qualité » du stockage des données se dégrade. Les données peuvent alors être dupliquées vers un autre boîtier neuf, tout en préservant leurs caractéristiques initiales, avec l'information supplémentaire qu'elles proviennent du boîtier « source ». On notera que la procédure de duplication peut être vérifiée par huissier (au sens du respect du mode opératoire défini par LexBOX ; il est peu probable qu'un huissier puisse faire la vérification au sens informatique du terme).

Exemples d'utilisation de LexSafe :

- gestion de la propriété intellectuelle (antériorité de données pour un brevet ; enregistrement en confiance ; conservation fiable de données)
- traçabilité d'opération ou de processus (audit de comptes)
- gestion de données à effacement programmé (journaux d'accès).

L'effacement programmé correspond à une durée de vie de la donnée. Au-delà, elle n'est plus accessible (« disparue ») mais n'est pas détruite. Elle peut donc être extraite du support, typiquement sur demande judiciaire.

Les équipements peuvent activer un sceau de chiffrement, auto-généré par l'équipement lui-même. Si ce sceau est « sorti » de l'équipement (par exemple pour fourniture à tiers de séquestre) avant l'activation définitive de l'équipement (cette extraction est impossible après l'activation de l'équipement), l'utilisateur a le moyen de savoir que sa clé a été extraite. A terme, il pourra savoir qui en dispose (qui a procédé à l'extraction).

Une présentation rapide de DesCryptor, disque dur chiffré (via de l'électronique spécifique) pour portable, a aussi été faite.

2. Présentation de LogManager

Présentation faite par M. Raymond Mercier. URL : http://lmcr.free.fr
Présentation : http://www.ossir.org/resist/supports/cr/20050926/LogManager.pdf

LogManager est un outil libre fonctionnant sous Windows, permettant la collecte, l'agrégation et l'analyse de journaux. Base technique : Windows, SQL Server/MySQL/MSDE. Le portage du collecteur vers Linux est en cours.

Quelques définitions :

- Journaliser : enregistrer des événements et des états.
- Etat : situation donnée, figée. Sorte de photographie à un instant donné.
- Evénement : différence entre deux états.

La conception et l'écriture de LogManager ont découlé des constats suivants, concernant le traitement des journaux :

- Il est nécessaire de prendre en compte des univers très différents (Unix/Syslog, Microsoft/EventLog, SNMP/traps, CheckPoint/LEA).
- La journalisation met en jeu des sources disparates (équipements réseau, systèmes, applications).
- Les journaux restent souvent dans leur domaine (les journaux réseau sont traités par l'équipe réseau, les journaux système par l'équipe système…).
- La corrélation est rare, le croisement des journaux l'exception. D'où des problèmes de détection d'incidents corrélés.
- Les journaux restent souvent sur le système qui les a générés.

LogManager se veut un fédérateur, afin d'améliorer et de faciliter la gestion des journaux. L'outil est composé de trois types d'entités :

- Agents : collecte et centralisation
- Base de données : stockage et accès
- Clients : traitement des données.

Les collecteurs/stockeurs sont organisés de façon arborescente : niveaux local, régional, national par exemple. Il n'existe pas encore de possibilité de remontée sélective entre deux niveaux, pour le moment la remontée fonctionne en tout ou rien : tout le niveau N est remonté au niveau N-1, ou rien n'est remonté.

Protocoles utilisés :

- VIPLog entre constituants de l'arbre LogManager.
- UDP sur le brin local, entre un agent et son collecteur
- TCP entre collecteurs. Les échanges TCP incluent une compression (LZW) et du chiffrage de l'échange (SSL).

Spécificités de VIPLog : chaque message est numéroté (pour la détection de pertes), horodaté (UTC) à l'émission, et contient les informations sur le thread/processus/utilisateur associé à la génération du message.

Protocole VIPRequest : interrogation du collecteur. Repose sur HTTP/HTTPS.

Composant EventCatch : transformation des EventLog (Windows) en VIPLog. Le composant doit être local à la machine sur laquel le message EventLog est produit : les DLL de « décodage » de ces messages sont propres à l'application qui les produit.

Performances maximales observées (sur un PIII 600Mhz, 128 Mo RAM, contenant « tout LogManager » : outils producteurs, base de données, collecteur) : 100 messages par seconde amènent le système à 100% de CPU.