

Opérations pilotes de protection et chiffrement de fichiers et données sensibles au CNRS

Journée des CRSSI - CNRS - 11 septembre 2008

Bernard Perrot, CNRS - UMR6205

<bernard.perrot@univ-brest.fr>

Contexte

- Démarrage d'une autre opération pilote de chiffrement de surface concernant les (nouveaux) portables.
 - pilotage et présentation à suivre de *François Morris*
- Cette opération traitera des "fichiers et données", sans que ce terme soit forcément techniquement limitatif, sauf à ne pas traiter le chiffrement de surface qui fait l'objet de cette autre opération !
 - concerne les données "sensibles" mais...
 - ... ne s'étend pas aux données classifiées (notion formelle) qui ont vocation à donner lieu à une approche (outils) spécifique dans un contexte rare au CNRS.
 - différent du chiffrement de surface, car celui-ci ne s'adresse qu'au problème de la confidentialité de données sur un support inactif (on est protégé du vol, mais

Contexte (Suite)

pas d'une intrusion machine en fonctionnement car tout le système d'exploitation a accès aux données une fois l'accès au support autorisé).

- **Cette opération fait suite à des précédente ainsi qu'à des travaux déjà réalisés, à réutiliser bien évidemment :**
 - **"groupe Jeannin"**
 - **expérimentations DR Midi-Pyrénées (*R. Dartiguepeyron*)**
 - **recommandations pour la protection des données et chiffrements (*F. Morris*)**
 - **diverses contributions dans "Sécurité Informatique"**
 - **...**

Le besoin

- **Le chiffrement est un outil (sans doute incontournable dans le cas présent), mais pas la fin en soi.**
- **une approche de type "analyse de risques" doit permettre l'identification des cibles (fichiers, données, partitions, ...) concernées et leur degré de sensibilité (on redoute qui et quoi.**
 - **on peut imaginer que sans que cette approche formelle ai déjà eu lieu, une conscience de détenir des données sensibles existe déjà pour certains, une analyse simplifiée permettra d'en déterminer plus formellement la nature et la sensibilité.**
- **les données étant identifiées, il est très important d'en connaître précisément le "cycle de vie" afin d'apporter une solution de protection adaptée :**

Le besoin (Suite)

- **données partagées ou pas entre plusieurs personnes ?**
- **localisées ou distribuées ?**
- **mono-support ou multi-support ? Monosite ou multi-sites ?**
- **si partagées, avec des personnes étrangères ou pas au CNRS ?**
- **modes d'échanges ?**
- **traitées par quel logiciels ?**
- **qualification sensible permanente (dossier médical) ou seulement temporaire (dossier de brevet) ?**
- **ou sont les copies, les sauvegardes, ...**
- **destruction**

Le besoin (Suite)

- **etc.**
- **la recommandation qui sera issue de cette opération pilote sera accompagnée d'une préconisation en matière d'outils et procédures à mettre en oeuvre.**
- **tenir compte de la diversité des situations concernées :**
 - **laboratoire, service administratif, ...**
 - **serveurs, postes de travail individuels, nomade ou pas, personnels ou pas, ...**
 - **systèmes d'exploitations divers, systèmes de fichiers divers, attachements divers (DAS/SAN/NAS), ...**

Les objectifs

Cette opération pilote a pour but d'éprouver le déploiement de solutions dans diverses configurations, et d'en tirer des enseignements :

- **sur les moyens humains et techniques nécessaires (technicité, formation) et l'accompagnement nécessaire (préalable, support, évolutions)**
- **sur les difficultés techniques éventuelles, incompatibilités**
 - **en particulier, compatibilité avec les techniques de chiffrement de surface faisant l'objet de l'autre opération pilote)**
- **sur le plan humain, facilité ou non de mise en oeuvre et d'appropriation de la méthode.**
- **sur le recouvrement (possible, facile à mettre en oeuvre).**

Les objectifs (Suite)

- **sur la réalité (l'efficacité) de la protection réalisée.**
 - **vérification autant que possible que le dispositif ne comporte pas de "faille" rompant la protection effective des données**
 - **si faille il y a, évaluation de la modification du risque encouru.**
- **sur les risques que la procédure fera courir aux données elles-mêmes (modification, altération, perte)**
- **sur les coûts et dépenses (supplémentaires) induites.**

Ces enseignements conduiront au constat final, de réussite ou d'échec, et sur les recommandations correspondantes.

Cette opération pilote :

Les objectifs (Suite)

- **permettra de tester des situations réelles et ajuster les recommandations.**
- **offrira des références (des exemples) réelles utiles aux déploiements futurs.**
- **permettra de disposer d'un échantillon d'experts formés à travers ces expérimentations.**

Configurations "cibles" à tester

- environnements Windows, MacOSX, Linux, Unixes
 - dont compatibilité de la solution en environnement collaboratif hétérogène !
- postes individuels, serveurs départementaux
- données partagées et non-partagées
- Bases de données
- dispositif d'échanges de données
 - en particulier, échanges par messagerie
- supports de stockages amovibles (clés USB et disques externe nomades notamment)
- cohérences et compatibilité avec les archives et sauvegardes des données concernées

Configurations "cibles" à tester (Suite)

- **laboratoire (expériences), services généraux (dont service informatique !), services administratifs (unité, DR, siège)**

Déroulement de l'opération

Au moins cinq expérimentations sont à prévoir.

L'opération pourrait se dérouler comme suit :

- **mise en place d'un groupe de pilotage**
- **rédaction du cahier des charges des expérimentations**
- **évaluation des coûts (et mode de financements...)**
- **appel à candidatures, et choix des expérimentateurs (acteurs, responsables informatiques, pilote local)**
- **définition plus précise avec les expérimentateurs des configurations et outils et méthodes**
- **soutien méthodologique et technique des expérimentateurs**
- **évaluation de chaque expérimentation**

Déroulement de l'opération (Suite)

- **bilan, recommandations**
- **élaboration d'un guide de la protection et du chiffrement des données et fichiers sensibles**

Planning

- **Constitution du groupe de pilotage : septembre 2008**
- **Appel à candidatures (hors IN2P3) : septembre 2008**
- **Cahier des charges des expérimentations et validation : octobre 2008**
- **Traitement des questions budgétaires : octobre 2008**
- **Définition des projets locaux et des équipes concernées : novembre 2008**
- **Formations collectives éventuelles : décembre 2009**
- **Lancement des opérations : début janvier 2009**
- **Déroulement, suivi : 1er semestre 2009**
- **Évaluation : juin-septembre 2009**

Planning (Suite)

- **Bilans – conclusions : septembre 2009**
- **Guide de recommandations « chiffrage » : novembre 2009**

Quelques réflexions personnelles...

Abordant juste le dossier, dans le désordre, quelques idées et pistes qui me traversent l'esprit... :

- **la plupart des acteurs et utilisateurs finaux (et en particulier au delà de l'opération pilote) ne devront pas être "perturbés" ni contraints outre mesure dans leur quotidien. Il faudra donc déboucher sur des procédures simples et compréhensibles, que les acteurs puissent s'approprier.**
- **malgré cela, il ne faudra pas exclure à priori que des situations particulières (matérielles, logicielles, organisationnelles) puissent être incompatibles avec l'objectif, et que des modes de travail devront alors être changés pour atteindre les objectifs (ne pas perturber les acteurs**

Quelques reflexions personnelles... (Suite)

dans leur quotidien ne veut pas dire ne pas commencer par modifier un mode de travail inadapté...)

- **l'usage des certificats n'a pas connu le développement que les promoteurs et informaticiens pouvaient supposer/espérer, s'en souvenir (trop compliqué ? à quoi ça sert ? Manque de possibilité/volonté de convergence entre partenaires ? ...)**
- **peut-être des difficultés issues de situation actuelle ? (pas de messagerie "unifiée" au CNRS, certificats CNRS inadaptés au chiffrement/recouvrement car durée de vie trop courte et pas de séquestre, ...).**
- **est-ce que des dispositifs matériels et/ou biométriques peuvent être utilisables (et profitables) pour atteindre**

Quelques reflexions personnelles... (Suite)

certains objectifs (clés USB par exemple, carte à puce, ...) ?

- **les recommandations et le guide final ne devront pas être rendues caduques ou impossibles à mettre en oeuvre sur simple modification des fournitures logicielles préconisées et présentes sur le marché (il faudra des logiciels, chiffrement en particulier, mais ne pas être trop tributaire de spécifications propres ou d'un fournisseur particulier)**
- **Il faudra répondre aux besoins d'environnements divers (Windows, Unix/Linux, MacOSX, ...), mais éviter tant que faire ce peut que cela débouche sur des recommandations et guides fondamentalement différents.**
- **en conséquence les solutions logicielles et méthodologies qui peuvent être communes (ou indépendante de**

Quelques reflexions personnelles... (Suite)

la plateforme) devront retenir particulièrement l'attention

- **porter une attention particulière aux "logiciels libres", souvent plus facile à s'approprier.**
- **et si un groupe expérimental était le groupe de pilotage lui-même ?**

Contact :

Bernard Perrot

`<bernard.perrot@univ-brest.fr>`

et le service du FSD.