Poste de travail léger sécurisé

Laurent CABIROL

Commissariat à l'Énergie Atomique,
Direction des Technologies de l'Information,
Bat 474 91191 Gif sur Yvette cédex
laurent.cabirol@cea.fr

Résumé Le Commissariat à l'Énergie Atomique se propose de déployer dans ses centres de recherche des applications nationales très fortement sécurisées dans un mode client-serveur. Après un rappel de la problématique, l'exposé décrira les règles qu'il s'impose pour la protection des informations sensibles manipulées par ces applications et les menaces contre lesquels il se propose de se protéger. Nous passerons ensuite à une description sommaire de la solution retenue basée sur un client léger Linux sans disque dur et avec lecteur de carte à puce utilisant un VPN pour communiquer avec le serveur. L'exposé s'attardera sur les mécanismes de boot, puis de chargement de système et d'applications en présentant différents choix possibles de sécurisation selon les étapes.

1 Contexte du déploiement d'applications sécurisées

Le CEA est un établissement public de recherche dont les laboratoires sont répartis au sein d'une douzaine d'établissement différent sur le territoire national. Ses recherches couvrent un champ assez vaste, des travaux nécessaires à la maîtrise de la production d'énergie nucléaire à la recherche fondamentale, notamment dans les domaines de la physique théorique et des sciences du vivant, en passant par des actions nombreuses de recherche technologique, par exemple dans le domaine des matériaux, de la micro électronique ou des nanotechnologies, sans oublier les travaux nécessaires au maintien de la capacité de dissuasion nationale. Le CEA regroupe environ 15000 salariés auxquels s'ajoutent de nombreux thésards, stagiaires et collaborateurs extérieurs (*http ://www.cea.fr/*).

Son parc informatique comprend environ 18000 postes de travail bureautique, de très nombreux serveurs de puissance variés et un centre de calcul à hautes performances. Touts ces ordinateurs sont reliés par un réseau très performant connecté à Internet via le réseau RENATER.

Pour le déploiement d'applications nationales (comme son système de gestion par exemple), le CEA a choisi d'utiliser un modèle d'architecture client-serveur et a établi des règles formalisées dans un recueil normatif interne (Normacs). Le CEA fait évoluer ce modèle pour prendre en compte les évolutions techniques (J2E, web services, portail, etc...).

Le déploiement d'applications sécurisées devra impérativement prendre en compte ce contexte dans une optique d'intégration plus rapide au moindre coût de ces applications au sein du système d'information du CEA.

2 Les menaces supplémentaires

Nous prenons pour hypothèse de travail que l'environnement informatique et réseau standard du CEA est à un niveau de sécurité conforme à l'état de l'art.

Par rapport aux applications standards déjà déployées, les applications fortement sécurisées doivent proposer des fonctionnalités supplémentaires pour prendre en compte de nouvelles menaces. Celles-ci sont détaillées dans la suite de ce papier. Nous ne décrivons pas les améliorations à faire ou à prendre en compte du coté "serveurs". Nous faisons l'hypothèse de travail qu'ils bénéficient d'une protection physique suffisante et de personnels d'administration sûrs.

2.1 Confidentialité des échanges

Les échanges entre les postes de travail et les serveurs centraux utilisent le réseau CEA. Même si le personnel intervenant au CEA fait l'objet de contrôle strict de sécurité, l'application plus rigoureuse de la règle du "*besoin d'en connaître*" impose une séparation du trafic de façon à ne pas permettre à un éventuel intrus de "sniffer" les échanges et de disposer d'informations qu'il n'aurait pas à connaître. Pour ne pas avoir à déployer un second réseau physique, il devient donc nécessaire de chiffrer les échanges entre client et serveur.

2.2 Authentification forte des utilisateurs des applications sécurisées

L'application stricte de la règle du "*besoin d'en connaître*" nous conduit également à vouloir authentifier de façon sûre l'utilisateur d'une application sécurisée. En effet, l'usage classique d'une authentification par "*login/password*" n'est pas jugé suffisamment forte dans ce contexte.

2.3 Protection physique du poste client

Les postes clients en ce qu'ils permettent l'accès aux applications sécurisées sont eux- même sensibles. Ils peuvent être volés afin de récupérer les informations qu'ils contiennent, que ces informations proviennent des applications elles-mêmes ou permettent par leur connaissance de les attaquer.

Il convient donc de protéger les postes de travail pour se prémunir de ce type d'attaque. La méthode classique consiste à établir un ou plusieurs périmètres de protection physique autour des ressources sensibles. Le coût de cette protection étant très élevé, il est nécessaire de le diminuer (et si possible de s'en affranchir) et donc de trouver des moyens de rendre le vol d'un poste de travail sans conséquence.

2.4 Intrusion dans le poste client

Disposer d'un poste client permet de l'étudier en détail et d'en déduire des informations qui permettrait de diminuer la sécurité du système. Des mesures prises en conséquence seront détaillées au chapitre suivant.

3 Éléments de solution

3.1 Authentification des utilisateurs

Le CEA dispose d'une infrastructure de gestion de clés et est à même de délivrer à ses personnels un certificat X509 stocké dans une carte à puce. Ce mode d'authentification sera donc imposé pour l'accès aux applications sécurisées. Le renforcement de l'authentification, et donc de la sécurité, vient de la nécessité de disposer d'un objet (la carte à puce) et de connaître le pin-code associé pour pouvoir accéder à ces applications.

3.2 Confidentialité des échanges

Pour répondre à la contrainte de chiffrement des échanges, nous mettons en place un VPN IPSEC. L'échange initial de clés se fera sous le contrôle du certificat X509 de l'utilisateur contenu dans sa carte à puce.

3.3 Protection physique, vol du poste de travail

Pour cela, nous nous imposerons de ne pas avoir de données rémanentes de l'application sur le poste de travail et donc de ne pas avoir de disque dur ou de dispositif de stockage amovible (disquettes, dongles USB, etc.).

3.4 Intrusion dans le poste client

Pour limiter les conséquences de la "possession" par un intrus d'un poste client sur la sûreté du système, des mesures anti-intrusion sont bien sûr mises en place sur le boîtier même du poste.

Nous nous sommes imposés de ne pas avoir de données rémanentes de l'application. Il faut cependant pouvoir « booter » le poste de travail de façon sûre. Deux possibilités s'offrent à nous : télécharger l'application de façon sécurisée ou démarrer le poste de travail à partir d'un dispositif non-réinscriptible (cd-rom). C'est ce dernier choix que nous avons fait. Il entraîne bien sûr des mesures supplémentaires pour la protection du dispositif qui stocke l'application, le système d'exploitation et ses données de configuration.

Dans ce contexte, il paraît aussi souhaitable de contrôler l'utilisation du poste client au plus tôt dans le processus de démarrage pour éviter les possibilités d'intervention "malicieuses" lors de cette phase sensible.

Nous choisirons ici de démarrer le poste de travail sous le contrôle d'une carte à puce d'administrateur. Cela permet de séparer ce rôle de celui de l'utilisateur. Afin que le vol du poste ne permette pas de récupérer d'informations sensibles sur sa configuration, nous avons choisi de chiffrer celles-ci sur le cd-rom. Le déchiffrement se fait sous le contrôle de la carte à puce d'administrateur. Une fois le poste démarré, l'utilisateur peut alors ouvrir une session à l'aide de sa carte personnelle (voir figure 1).

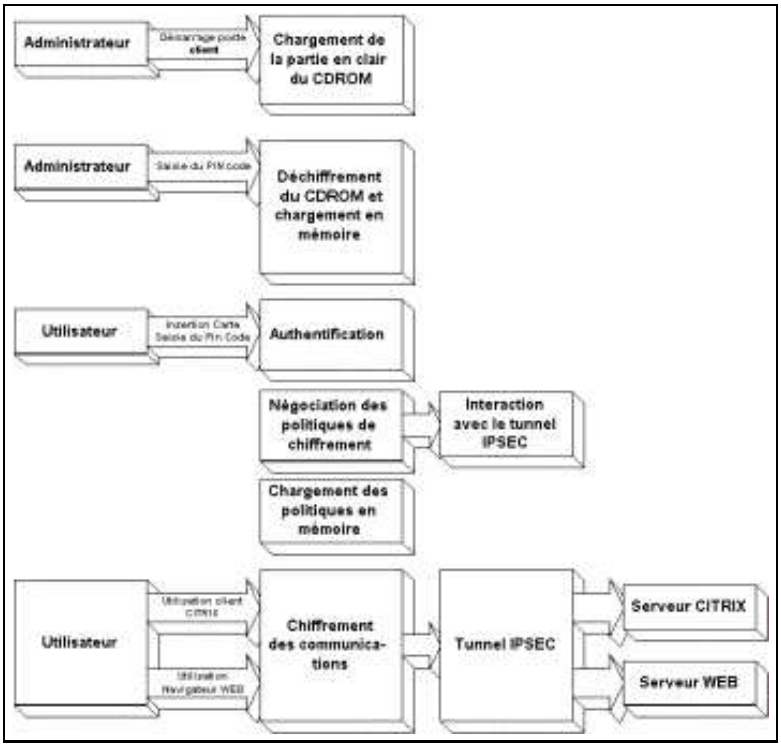

Fig. 1. Démarrage du poste de travail

4 Choix techniques

4.1 Matériel

Le poste de travail est constitué d'un PC standard auquel sont ajoutés un dispositif d'anti-intrusion, un lecteur de carte à puce avec clavier intégré. Cela permet de limiter le coût du matériel.

4.2 Logiciel

Le logiciel est constitué d'un système d'exploitation Linux configuré avec les seuls modules utiles et compilé spécifiquement pour ce PC après application des patchs de renforcement de la sécurité. Le mécanisme d'initialisation est spécifiquement modifié pour prendre en compte une authentification par carte à puce d'un administrateur avant le démarrage des services "réseau". Deux versions sont créées, l'une avec un client CITRIX, l'autre avec un navigateur standard.

4.3 Processus de démarrage du PC

Le mécanisme de boot du PC n'a pas été modifié. Le souhait de pouvoir contrôler l'utilisation du poste client au plus tôt dans le processus de démarrage (dès le boot) a conduit à examiner plusieurs choix possibles détaillés ci-après.

L'authentification au plus tôt lors du démarrage du PC impose de pouvoir ajouter des fonctionnalités supplémentaires comme la possibilité de dialoguer avec une carte à puce, de déchiffrer les informations de configurations du poste de travail, etc. Cela conduit à souhaiter l'extension soit du BIOS, soit du chargeur.

4.4 Modification de la ROM du BIOS du PC

Plusieurs possibilités existent pour remplacer le BIOS "standard" d'un PC, à savoir :

- Openfirmware,
- Linuxbios,
- Freebios.

La forte dépendance au matériel (chipset) de ces solutions ne permet pas de les envisager sans un effort jugé trop important à ce stade de notre projet.

4.5 Modification d'un chargeur

Les nombreux chargeurs du monde "propriétaires" n'ont pas été regardés pour des raisons évidentes de non-disponibilité des sources.

Dans le monde "libre", trois chargeurs principaux se partagent le "marché", à savoir :

- Syslinux/isolinux,
- LILO,
- GRUB.

La modification d'un chargeur pour des raisons équivalentes à la modification du BIOS n'a pas été retenue.

4.6 Modification de la procédure d'initialisation LINUX

Cette procédure a été modifiée afin de permettre l'authentification de la carte "administrateur" pendant son déroulement, et ainsi permettre le déchiffrement des informations confidentielles spécifiques du poste de travail et du réseau. Sont ensuite lancé directement le client nécessaire ainsi que le tunnel IPSEC après l'authentification réussi de l'utilisateur au moyen de son certificat X509 stocké sur sa carte à puce.

4.7 Quelques mesures de sécurité complémentaires

D'autres mesures ont été retenues de façons à rendre plus difficile le succès d'une attaque du poste client. Elles ne seront pas exposées. A titre d'exemple cependant, un mécanisme de couplage/identification réciproque du CD, du PC et de la carte administrateur a été mis en place.

5 Quelques exemple de scenarii malveillants

5.1 Vol du CD de démarrage

Les informations réellement importantes sont chiffrées sur le CD et donc inaccessibles. Le reste est du domaine public.

5.2 Démarrage du PC avec un autre CD

Cela nécessite l'ouverture du PC et donc la mise en œuvre des mesures anti-intrusion matérielles (blocage du boot du PC). Quand bien même, celles-ci seraient mise en défaut, l'attaquant devrait alors mettre en défaut le boîtier VPN protégeant les serveurs et serait repéré par le système de détection d'intrusion coté "serveurs".

5.3 Vol d'une carte "administrateur"

Il faudrait voler en plus le pin code de la carte. L'administrateur n'a pas pour autant l'autorisation de se connecter aux applications, il faudrait aussi voler une carte utilisateur et son pin code. Par ailleurs, il n'y a pas de "*shell*" sur le poste de travail, juste le client CITRIX ou le client WEB.

6 Conclusions

Les mesures rapidement décrites précédemment permettent de se protéger :
- de l'utilisation par des personnels non autorisés,
- de l'écoute sur le réseau,
- de l'intrusion sur le poste de travail,
- de limiter les conséquences d'un vol du poste de travail.

L'utilisation de composants "libres" permet de construire le poste client léger souhaité à moindre coût en prenant en compte les contraintes de sécurité que nous nous sommes fixées.

Références

1. BIOS
   http ://www.openfirmware.org/
   http ://www.linuxbios.org/
   http ://freebios.sourceforge.net/

2. Loader
   http ://syslinux.zytor.com/
   http ://brun.dyndns.org/pub/linux/lilo/
   http ://www.gnu.org/software/grub/
   bibitemlinux Linux
   http ://diet-pc.sourceforge.net/
   http ://www.linuxfromscratch.org/

3. Cartes à puce et Linux
http ://www.linuxnet.com/