L'usage des logiciels libres dans les systèmes informatiques critiques, répond-il aux impératifs de sécurité et de sûreté ?

Emile Geahchan
Responsable thématique du projet Plume du CNRS
Professeur au Cnam de Versailles
Enseignant à l'Université d'Evry

PROLOGUE

- Eric Raymond - un des pionniers du logiciel libre - ne peux s'empêcher de manifester son enthousiasme devant les avancées des communautés Linux :

  « Linux est subversif. Qui aurait imaginé, il y a seulement cinq ans, qu'un système d'exploitation de classe internationale prendrait forme comme par magie a partir de bidouilles » (1998).

- Il est intéressant de comparer cette citation à celle plus sombre de Frederick Brooks concepteur de l'OS multitâche de l'IBM-360 :

  « Le bourbier de la technique du logiciel subsistera longtemps encore. On peut penser que la race humaine continuera à réaliser des systèmes se situant aux limites de ses possibilités ; et les systèmes logiciels sont peut-être les plus compliqués et les plus complexes des travaux humains ... » (1975).

INTRODUCTION

- Les entreprises sont généralement frileuses en ce qui concerne l'utilisation des logiciels libres. Elles s'interrogent quand à la confiance à accorder à ces logiciels et aux organisations qui les soutiennent. Elles ont tendance à n'attacher de valeur qu'aux garanties contractuelles offertes par les grands éditeurs de logiciels propriétaires.

  Cette frilosité des entreprises va parfois jusqu'à la méconnaissance totale du marché du logiciel libre.

- Les chercheurs et les enseignants sont naturellement plus enclins à s'intéresser aux logiciels libres. Ils tirent profit de ce nouveau marché, par souci d'économie certes, mais aussi parce que ces logiciels possèdent certaines caractéristiques intéressantes, liées à leur cycle de développement :
  - la transparence liée à l'accès direct au code source,
  - la maîtrise du logiciel, dans le sens de la non-dépendance,
  - la synergie des communautés de concepteurs-développeurs,
  - la disponibilité qui en résulte.

INTRODUCTION

- Ces caractéristiques vont donner aux logiciels libres un certain nombre d'atouts quand aux exigences de sécurité et de sûreté des systèmes critiques, exigences que je centrerai sur les critères suivants :
  - La Fiabilité : Continuité du service fourni.
  - La Maintenabilité : Possibilité de réparation et d'évolution du système.
  - La Pérennité des investissements : Conditions et durée de la Maintenance maîtrisée.
  - La Sécurité : Résistance aux attaques.

- Mon objet est de vous proposer une "réflexion" aidant à envisager l'introduction de logiciels libres dans la panoplie des composants de confiance de votre entreprise. Cette réflexion est le résultat de nombreux échanges avec mes collègues du Cnam, de l'Université d'Evry, du CNRS, de l'IMdR (GTR64), tous des acteurs expérimentés, dont les auditeurs du Cnam en formation professionnelle et qui possèdent une expérience de terrain et de réflexion.

LES LOGICIELS LIBRES

- Un "logiciel libre" est un logiciel dont l'utilisation, l'analyse, la modification et la diffusion sont autorisées techniquement et juridiquement :

  - Techniquement par la disponibilité du code source.

  - Juridiquement grâce à des licences spécifiques, dont les plus connues sont la licence GPL de la Free Software Foundation et la licence BSD de l'Université de Berkeley.

GPL (General Public Licence) dont la caractéristique est que tout logiciel dérivé doit obligatoirement adopter la licence GPL elle même -> Exemple le noyau de Linux

BSD (Berkeley Software Distribution) dont la caractéristique est qu'un logiciel dérivé peut être protégé par des droits d'auteur (logiciel propriétaire) -> Exemple Mac OS X

Free Software Foundation : Infrastructure légale pour la communauté du logiciel libre, fondée en 1985 par Richard Stallman - un des pionniers du logiciel libre.

CeCILL (CEa Cnrs Inria Logiciel Libre) licence élaborée en France par

I- La Fiabilité

- Les grands logiciels libres professionnels, Serveurs Linux, Serveurs Web Apache, Messageries et autres outils réseaux, sont majoritaires sur l'Internet et ne semblent pas soulever de problèmes particuliers quand à leur fiabilité.

- La grande majorité des langages de programmation sont disponibles en logiciel libre :

C /C++ Java Objective-C

PHP Python Perl Ruby

I- La Fiabilité

-
- PROMOUVOIR LES LOGICIELS UTILES MAÎTRISÉS ET ECONOMIQUES DANS L'ENSEIGNEMENT SUPÉRIEUR ET LA RECHERCHE

- 371 logiciels sont utilisés aujourd'hui par la communauté Plume du CNRS, il s'agit de logiciels correspondant à différents besoins ,de la gestion administrative aux calculs mathématiques en passant par la sécurité des systèmes.
- Ces logiciels ne semblent pas soulever de problèmes particuliers quand à leur fiabilité.

www.projet-plume.org

II- L'Assistance

- L'assistance est un point délicat à résoudre en matière de sécurité du logiciel. De fait le client a besoin d'être en confiance avec ses propres fournisseurs à savoir ses éditeurs. On peut trouver parmi eux Microsoft, IBM, Oracle, SAP etc. de grandes marques qui par définition laissent supposer au client qu'il sera en sécurité. Cependant cette assistance renforce sa propre dépendance par rapport à ces éditeurs.

- Dans le cadre du logiciel libre l'indépendance peut paraitre moindre dans un premier temps, mais elle devient de plus en plus forte par la suite : Il existe dans la communauté des utilisateurs de logiciels libres, des services d'assistance qui nécessitent un apprentissage ; avec le temps les procédures acquises en interne et avec les communautés du logiciel libre font que l'on devient de plus en plus indépendant et que l'on maîtrise de plus en plus la sécurité de ses propres systèmes.

  C'est là la démarche asymptotique de la sécurité acquise avec le logiciel libre.

III- La Documentation

- L'ingénieur de maintenance qui veut effectuer du "tuning" (ou d'autres tâches complexes) sur les grandes bases de données relationnelles propriétaires du marché, éprouve de grandes difficultés à réaliser les fonctions élémentaires requises en se basant sur la documentation fournie par l'éditeur et se trouve généralement dépendant des services d'assistance : Les éditeurs ne délèguent pas facilement la maîtrise de leur systèmes.

- L'avantage revient au logiciel libre, la documentation est mieux structurée et plus complète. Elle s'améliore au fur et à mesure de l'avancement des logiciels puisque les sources sont disponibles. Par exemple la communauté des développeurs Java se retrouve complètement dans la documentation support

IV. La Maintenance Préventive et Corrective

- On assiste à une validation permanente des logiciels libres par les communautés du Logiciel Libre et la communauté scientifique en général : Le code source est lu, relu, testé dans des contextes très différents par des chercheurs, enseignants, étudiants et passionnés du monde entier.

- Comme le dit Eric Raymond :

  « Étant donné un ensemble de bêta-testeurs et de co-développeurs suffisamment grand, chaque problème sera rapidement isolé, et sa solution semblera évidente à quelqu'un ».

- Andrew Wiles a soumis sa démonstration du grand théorème de Fermat à certains de ses collègues et de ses étudiants, des erreurs on été découvertes puis corrigées et grâce à ce travail d’équipe la démonstration complète a pu être publiée en 1994. Aujourd'hui de plus en plus de théorèmes sont élucidés par des communautés scientifiques.

V- La Maintenance Evolutive

- Les éditeurs possèdent un service Marketing, ils devraient normalement répondre aux besoins de leurs clients, mais cela reste à composer avec le schéma directeur de l'entreprise et les contraintes de son organisation interne.

- Lorsqu'un nouveau besoin apparait, il est souvent plus facile d'y répondre avec les logiciels libres, la transparence des sources rend les évolutions toujours possibles d'une façon ou d'une autre.

Smartphones

La majorité des Smartphones fonctionnent aujourd'hui sous l'OS Androïd (logiciel dérivé de Linux). Les Smartphones équipés d'Androïd ont été plus réactifs que les Smartphones équipés des versions "Mobile" de Windows pour contrer l'iPhone d'Apple.

VI- La Pérennité

La pérennité est l'assurance de la continuité de service sur le long terme.

- Les Entreprises sont particulièrement dépendantes des éditeurs dans le domaine des systèmes informatiques, cette dépendance est illustrée par cette statistique du Clusif :

  « en 2010, 80% des Grandes Entreprises Françaises déclarent être fortement dépendantes de leur Systèmes d'Information » .

- Les éditeurs font évoluer leurs logiciels à leur guise, par exemple :
  - Le passage de Windows XP à "Vista" qui n'a jamais convaincu les Entreprises.
  - L'arrêt pur et simple par les éditeurs de la maintenance de leurs logiciels ou de certains modules de leurs logiciels.

- Enfin éventualité à prendre en considération : Les éditeurs peuvent disparaitre.

VI- La Pérennité

- Dans le cas des logiciels libres, il y a le plus souvent une communauté qui se crée pour le "sauvetage" des logiciels libres ou même celui des logiciels propriétaires lorsque cela est possible, par exemple :

  - La communauté Mozilla Firefox fait revivre le navigateur Netscape.

  - La base de données relationnelle Ingres, en perte de vitesse est relancée en licence GPL sous le nom de PostGres (Post-inGres).

  - Après le rachat de Sun par Oracle et les tensions entre Oracle et la Free Software Foundation, une communauté reprend la suite bureautique OpenOffice sous le nom de LibreOffice.

- C'est ainsi que dans tous les cas le code source est toujours disponible.

VII- La Sécurité

- La sécurité des systèmes informatiques est toujours préoccupante, car dans ce domaine l'avantage est à l'attaquant et les vulnérabilités augmentent avec l'ouverture, notamment les réseaux.

- On assiste à une relecture permanente des logiciels libres par les différentes communautés, cela permet la détection des vulnérabilités et des éventuels chevaux de Troie. Ces contrôles ne peuvent évidemment pas être effectués dans le cas des logiciels propriétaires dont le code source est opaque et la rétro-ingénierie interdite.

- C'est le système d'exploitation "Scientific Linux" qui est implémenté sur la majorité des calculateurs du CERN, du CEA et des grilles de calcul française et européenne, cela en relation avec les centres de recherche internationaux aux USA en Chine e n Inde et au Japon ; comme en mathématiques il existe une recherche internationale sur la sécurité et la sûreté de Linux.

VII- La Sécurité

- La grande majorité des algorithmes de chiffrement du domaine public est disponible en logiciel libre :

  AES - Twofish - RSA - DSA

- La grande majorité des protocoles de sécurité des systèmes d'information est disponible en logiciel libre :

  OpenSSL - OpenSSH - OpenVPN - OpenRadius - OpenPGP

- La liste des virus connus est centralisée et maintenue par la communauté **WildList** (the Wildlist Organisation International)

- La liste des vulnérabilités connues est centralisée et maintenue par la communauté **CERT** (Computer Emergency Response Team de l'université de Carnegie Mellon).

VII- La Sécurité

Les mises à jour critiques

- Tous les ans des milliers de failles de sécurité sont découvertes tous logiciels confondus. Ces failles sont corrigées au fur et à mesure et les corrections sont diffusées sous la forme de mises à jour dites critiques.
- Ces mises à jours critiques créent une nouvelle problématique en matière de sécurité : La confiance dans les procédures de diffusion correspondantes.
- Dans le cas des logiciels propriétaires on se retrouve dépendants des procédures opaques mises en place par les éditeurs.
- Dans le cas des logiciels libres comme nous l'avons déjà expliqué dans le cas de l'Assistance, cela réclame une implication plus forte de l'entreprise au départ, mais ensuite on maîtrisera de plus en plus ces procédures.

EN TERMES DE REFLEXION

In fine la sécurité du logiciel ne sera-telle pas de mieux en mieux assurée grâce à la communauté scientifique, travaillant elle même sur les fondements du logiciel libre ?

- Au regard des avantages des logiciels libres présentés dans cette étude, je pense pouvoir affirmer que :

  1) Le niveau de maturité des logiciels libres est aujourd'hui au moins égal àcelui "réel ou prétendu" des logiciels propriétaires notamment dans les domaines de la Sécurité et de la Sûreté.

  2) Les Entreprises devraient commencer à envisager l'utilisation du logiciel libre, cela demandera la mise en place de structures collégiales capables :

  - d'une part de communiquer avec les communautés du logiciel libre,

  - d'autre part d'assurer les indispensables services d'assistance et dedistribution des mises à jour.

La majorité des Supercalculateurs Européens fonctionne sous Linux.