

Les enjeux juridiques du développement des TIC

Sécurité informatique des usagers :

l'apport des logiciels libres ¹

Vu Do Quynh ²

Responsable du Campus numérique francophone de Hanoi

Sommaire

Introduction.....	<u>1</u>
L'ordinateur individuel.....	<u>1</u>
La sécurité du poste informatique.....	<u>2</u>
Quelles sont les motivations liées à la diffusion de ces programmes malveillants ?.....	<u>3</u>
Les mesures de sécurité préventive les plus communes.....	<u>3</u>
Des risques à limiter pour l'utilisateur final.....	<u>3</u>
Malgré tout une pratique demeure, qui est pleine de risques.....	<u>4</u>
Quelques éléments sur la gravité des infections de virus informatiques au Vietnam.....	<u>4</u>
Les logiciels libres et leur contribution au problème de la sécurité du poste informatiques.....	<u>5</u>
Le projet GNU et le noyau Linux.....	<u>5</u>
Des caractéristiques intéressantes pour les utilisateurs finaux.....	<u>6</u>
Avec de tels avantages, comment se fait-il que le système GNU/Linux ne soit-il pas davantage répandu ?.....	<u>7</u>
Références.....	<u>7</u>

Introduction

Après avoir été contacté par la Maison du Droit pour faire une présentation sur les logiciels libres au colloque sur les enjeux juridiques du développement des TIC et après avoir constaté que le panel auquel je devais participer traitait de la cyber-criminalité, j'ai donc décidé d'orienter mon intervention sur le rôle que pouvaient jouer les logiciels libres dans la sécurité informatique du poste de travail de l'utilisateur final. En effet, selon moi, l'un des enjeux de la lutte contre la cyber-criminalité grandissante consiste à pouvoir assurer au mieux la sécurité du poste individuel contre toutes les attaques et toutes les intrusions visant à prendre le contrôle à distance du poste connecté à internet pour des buts litigieux.

Nous aborderons donc le problème de sécurité informatique du poste individuel tel qu'il se pose pour un utilisateur vietnamien ordinaire, tout d'abord en tentant de résumer le concept de sécurité informatique, puis de revoir rapidement les principales sources d'insécurité, les méthodes d'attaque, les mesures de protection et leur efficacité, pour enfin présenter l'apport potentiel des logiciels libres à la résolution de ces problèmes de sécurité.

L'ordinateur individuel

Pour fonctionner, tout ordinateur a besoin d'un système d'exploitation (SE), sans SE l'ordinateur

1 Présentation orale faite au Colloque "Les enjeux juridiques du développement des technologies de l'information et de la communication État des lieux et perspectives" organisé par la Maison du Droit vietnamo-française à Hanoi, les 17 et 18 novembre 2009.

2 courriel: vu.do.quynh@auf.org

peut s'allumer mais n'ira pas plus loin. Les principaux SE pour ordinateurs individuels rencontrés dans le monde sont [1], [2]:

- Microsoft Windows, qui est largement majoritaire avec plus de 90% des ordinateurs individuels, un chiffre probablement proche de 98-99% pour le Vietnam,
- Mac OS X, installé sur 3-6% des ordinateurs individuels,
- GNU/Linux, installé sur 1% des ordinateurs individuels.

La sécurité du poste informatique

Assurer la sécurité d'un poste de travail informatique consiste avant tout à pouvoir assurer l'intégrité de ce poste à différents niveaux qui sont:

- celui du SE : s'assurer que les fichiers qui constituent le cœur du SE restent intacts et ne soient pas corrompus ou effacés intentionnellement ou non;
- le besoin de prévenir l'intrusion de programmes mal-intentionnés, que nous appellerons par le terme générique de « malwares », par diverses manières : action humaine directe, par le biais de différents vecteurs comme la messagerie électronique, des pages web piégées, des cédéroms et des clés USB infectés;
- le besoin de préserver l'intégrité et la confidentialité des données personnelles stockées sur le poste informatique.

Parmi les principaux facteurs qui peuvent conduire à la compromission de la sécurité d'un poste informatique figurent [3] :

- l'utilisateur du poste lui-même, par manque de connaissance des règles de sécurité de base, ou par manque de volonté (voire la paresse) de les appliquer rigoureusement, ce qui peut conduire à l'installation à l'insu de l'utilisateur de programmes malveillants ou de leur activation ;
- la présence de failles de sécurité non corrigées au sein du SE et des applications fonctionnant sous le SE.

Les principaux programmes malveillants sont les suivants [3] :

- Le logiciel espion (spyware)
- Le virus
- Le ver (worm)
- L'enregistreur de frappe des touches du clavier (keylogger)
- Le wabbit
- Le cheval de Troie (trojan)
- L'exploit (de sécurité)
- Le rootkit
- La porte dérobée (backdoor)

L'infection du poste informatique par ces divers programmes malveillants se fait de diverses façons. Il s'agit pour l'auteur des programmes malveillants d'inciter l'utilisateur à ouvrir des fichiers infectés : des documents de travail au format .doc contenant des « virus macros » (petits programmes qui permettent de faire des opérations précises à l'ouverture du document), des fichiers infectés ou des fichiers de virus déguisés en fichiers de type image, son, etc., attachés à des courriers électroniques ; de le diriger vers des sites web qui exploiteront les failles du navigateur web pour installer sur le poste distant des programmes malveillants à l'insu de l'internaute.

Les postes infectés vont ensuite concourir, selon le type de virus, à infecter d'autres ordinateurs via le réseau interne ou via des systèmes de fichiers connectés temporairement à l'ordinateur infecté,

comme lors de la création d'un cd-rom, en infectant le secteur d'amorçage, ou au moment de l'insertion d'une clé USB. L'effacement ou la modification de fichiers nécessaires au bon fonctionnement du SE peuvent conduire à la paralysie du poste infecté et à l'impossibilité de travailler ou d'exploiter ses données par l'utilisateur. L'installation de programmes de type « porte dérobée » ou « rootkit » permet notamment de prendre le contrôle de l'ordinateur infecté à distance, par internet quand l'ordinateur y est connecté. Ceci permet à des individus sans scrupules de se constituer des « troupes » d'ordinateurs « zombies » qui pourront alors être utilisés au moment voulu pour attaquer en masse les serveurs publics appartenant à des compagnies dans le but de nuire à l'activité en ligne de ces dernières.

Quelles sont les motivations liées à la diffusion de ces programmes malveillants ?

Si au tout début, il s'agissait de démontrer un certain « savoir-faire », les attaques par des programmes malveillants sont, de nos jours, le plus souvent motivées par des aspects pécuniaires. Il s'agit par exemple de « vendre » aux victimes des programmes (ransomware) permettant de débloquent des ordinateurs au SE paralysé ou de décrypter des données rendues inaccessibles à la suite d'un chiffrement secret par le programme malveillant. Les formes d'escroquerie répandues sur internet consistent également à récupérer les données d'identité et les mots de passe des comptes bancaires trouvés sur les disques durs des ordinateurs compromis, soit pour les utiliser pour un profit personnel, soit pour les revendre à d'autres personnes peu scrupuleuses.

Les mesures de sécurité préventive les plus communes

Les usagers disposent de plusieurs outils, gratuits ou payants, pour essayer de garantir la sécurité de leur poste informatique. Il leur faut entre autre installer :

- un logiciel pare-feu (firewall) afin d'empêcher les intrusions externes, depuis internet, sur le poste informatique;
- un logiciel anti-virus afin de scanner automatiquement les fichiers envoyés par internet et, s'il est résident en mémoire de l'ordinateur, de détecter les activités virales déclenchées lors de la connexion de systèmes de fichiers informatiques externes infectés.

Par ailleurs, il est également nécessaire de procéder à la mise à jour régulière du SE et des applications afin de combler à temps les trous de sécurité qui ont été découverts.

Cependant, malgré toutes ces précautions, c'est souvent la course permanente entre les créateurs de nouveaux virus et les logiciels anti-virus. En plus, en ce qui concerne les logiciels dont le code source est fermé, il faut le plus souvent attendre que le concepteur du logiciel ait pu rendre public le patch de sécurité pour combler les trous de sécurité découverts dans son logiciel, ce qui peut parfois prendre du temps. Pour les logiciels dont le code source est ouvert, le temps entre la découverte du trou de sécurité est la mise à disposition du patch de sécurité correspondant est souvent très court, en particulier pour les logiciels open source qui disposent d'une communauté nombreuse et active.

Des risques à limiter pour l'utilisateur final

Étant donné que rien n'est sûr à 100%, pour limiter au maximum les risques d'infection de l'ordinateur, il existe des règles de prudence à observer :

- Éviter de télécharger des fichiers depuis ou de visiter des sites à haut-risque, comme les sites à caractère pornographique, les sites de téléchargement de chansons et de films peer-to-

peer ;

- éviter de télécharger des logiciels commerciaux payants qui ont été craqués ou des programmes de déblocage, qui peuvent être soit infectés soit être eux-même des virus déguisés ;
- toujours scanner les fichiers reçus par la messagerie électronique ou téléchargés depuis internet avec un ou plusieurs programmes anti-virus ;
- toujours vérifier l'adresse URL des sites pointés par les liens hypertextes contenus dans le corps des courriers électroniques, surtout si ces derniers sont reçus au format HTML.

Pour opérer des transactions en ligne, paiements ou transactions bancaires, il faut s'assurer que le site de paiement ou de transaction bancaire utilise bien un protocole sécurisé, comme *https* qui chiffre les données transmises par internet, et que le certificat d'authenticité du site est bien valide. Il faut bien entendu utiliser un navigateur internet dont les failles de sécurité aient été corrigées et qui soit performant sur le plan de la sécurité. Enfin, il est souhaitable de s'assurer que l'ordinateur utilisé pour exécuter les transactions bancaires n'ait pas été infecté par des programmes malveillants. Pour cela, la possibilité d'utiliser des SE installés sur cédérom bootable (live CD) est un avantage certain qui est rendu possible par l'utilisation des logiciels libres comme le SE GNU/Linux que nous verrons plus loin.

Malgré tout une pratique demeure, qui est pleine de risques

L'une des recommandations à suivre pour travailler sur un poste, surtout quand celui-ci est connecté à internet, est de ne pas travailler avec un compte ayant pouvoir d'administration. En effet, si quelqu'un ou un programme malveillant arrive à s'introduire sur le poste connecté, cette personne ou ce programme pourra hériter des droits de l'utilisateur connecté à la machine. Donc si l'utilisateur possédait les droits d'administration complète de l'ordinateur, tels seront les privilèges acquis par la personne ou le programme intrus. Cependant le SE le plus répandu sur les ordinateurs individuels autorise de créer à volonté des comptes d'utilisateur avec pouvoir d'administration et, comme il faut posséder les droits d'administration pour installer de nouvelles applications sur l'ordinateur, en conséquence la grande majorité des utilisateurs de ce SE travaillent tout naturellement avec des comptes à pouvoir d'administration, ce qui conduit forcément à des risques aggravés.

Quelques éléments sur la gravité des infections de virus informatiques au Vietnam

Selon le centre *Bach Khoa Information Security* (BKIS), une autorité reconnue dans le domaine des logiciels anti-virus conçus au Vietnam, il y aurait eu plus de 30.000 nouveaux virus ou variantes de virus détectés au Vietnam en 2008 [4], parmi lesquels 38 seraient d'origine vietnamienne. Le nombre d'infections virales sur des ordinateurs vietnamiens aurait totalisé 59 millions d'infections, toujours en 2008. Rien qu'à lui seul, le virus *W32.SecretW.Worm* aurait infecté 420.000 ordinateurs. Le mois de septembre 2008 détient le record avec plus de 3.500 nouveaux virus découverts dans ce mois [5], soit une moyenne de 120 nouveaux virus par jour. Dans le même mois, plus de 35.000 ordinateurs auraient été bloqués dans les mises à jour de sécurité de leur SE Windows. Les pertes économiques causées par ces infections de virus informatiques s'élèveraient à 2.400 milliards de dôngs (de l'ordre de 100 millions d'euros) en 2007. En 2008, ces pertes auraient été multipliées par un facteur 10.

En 2009 la situation de la sécurité du poste informatique individuel semble encore empirer avec, toujours selon BKIS, 15.000 nouveaux virus et 21,5 millions d'infections au cours des 4 premiers

mois de 2009? Nous apprenons aussi de BKIS que 97% des ordinateurs suivis par BKIS ont été infectés au moins une fois, que 90% des ordinateurs ont du réinstaller leur SE Windows et que les clés USB sont le principal vecteur d'infection par les virus informatiques [6]. En moyenne, sur les 4 premiers mois de 2009, les pertes économiques liées aux virus informatiques atteindraient en moyenne 327 milliards de dongs (de l'ordre de 15 millions d'euros) par mois [6].

Une étude de l'*Internet Storm Center* indiquerait que le temps moyen pour qu'un ordinateur non protégé ou disposant de failles importantes de sécurité non comblées puisse se faire infecter serait de l'ordre de 4 minutes [7]. Autant dire, que tout ordinateur devant se connecter à internet pour télécharger un patch de sécurité risque fort de se faire infecter avant même d'avoir eu le temps de télécharger le patch de sécurité en question.

L'augmentation rapide et importante du nombre d'internautes au Vietnam ces dernières années, selon le VNNIC il y aurait 25 millions d'internautes et 2,5 d'abonnés haut-débit ADSL en juin 2009 [8], fait du Vietnam un lieu propice pour « recruter » des ordinateurs zombies en vue d'actions cyber-criminelles. En effet, la plupart des logiciels installés sur les ordinateurs personnels des Vietnamiens sont des logiciels piratés, donc illégaux, dont la source est obscure. Une grande partie des petits magasins d'informatique dans certaines rues de Hanoi, par exemple, ont leur ordinateurs infectés, ce qui fait que tous les services numériques qu'ils peuvent rendre à leurs clients, comme le formatage d'un nouveau disque dur vendu résultera en un disque rendu au client et déjà infecté à l'insu de ce dernier.

Force est donc de constater que pour pouvoir protéger un poste individuel opérant sous le SE le plus répandu actuellement de toute tentative d'intrusion à caractère malveillant, il faut pouvoir déployer une somme d'énergie coûteuse en temps, pour appliquer toutes les procédures de vérifications des fichiers reçus, et en argent, pour l'achat des licences de logiciels dont celles pour les anti-virus sont annuelles, pour, au bout du compte, ne pas être garanti à 100% contre tout risque d'infection.

Il existe cependant d'autres SE pour lesquels cette menace d'infection par les virus informatiques est actuellement plutôt négligeable. Nous citerons ici le cas du SE Mac Intosh, de la marque Apple, et celui du SE GNU/Linux, tous les deux basés ou proches du SE Unix qui existe de longue date. GNU/Linux nous apparaît particulièrement intéressant pour le Vietnam puisqu'il est libre et, de surcroît, gratuit. Ceci le met à la portée de toutes les bourses tout en apportant une solution efficace et simultanée au problème du respect des droits intellectuels et de celui de la sécurité informatique du poste individuel, ce que nous allons aborder maintenant.

Les logiciels libres et leur contribution au problème de la sécurité du poste informatiques

Il est nécessaire, avant d'aller plus loin dans notre exposé, de présenter très rapidement ce qu'est un logiciel libre, leur origine et ce que l'on entend par l'adjectif « libre » ?

Le projet GNU et le noyau Linux

C'est en 1984 qu'un informaticien américain travaillant au *Massachusetts Institute of Technology*, appelé Richard Stallman, initia ce qu'il a appelé le projet GNU (*GNU is not Unix*) [9] dont le but est de créer un nouveau système d'exploitation, basé sur Unix, mais qui soit libre. Cette notion de liberté du logiciel se manifeste à travers la licence de distribution du logiciel libre *GNU General Public license* (GNU GPL [10]) qui garantit à l'utilisateur du logiciel 4 libertés fondamentales qui sont :

- la liberté d'utiliser en toutes circonstances le logiciel, y compris celle de le copier et de le distribuer

- la liberté d'étudier le fonctionnement du logiciel, donc de disposer d'un code ouvert,
- la liberté de modifier à sa convenance le logiciel,
- la liberté d'améliorer le logiciel en le redistribuant avec les modifications apportées.

Le système d'exploitation libre GNU que voulait développer Richard Stallman manquait cependant d'un noyau opérationnel, son noyau, appelé Hurd, étant toujours à l'état de développement, même encore de nos jours. Le noyau d'un système d'exploitation est la partie logicielle qui permet de gérer les périphériques et de les faire interagir avec la couche des applications fonctionnant sous le système lui-même. Cependant, en 1991, un jeune étudiant finlandais du nom de Linus Torvalds mit à la disposition du public un noyau de système d'exploitation (qu'il avait développé pour le système d'exploitation Minix, un clone d'Unix). Ce noyau, baptisé Linux, fut rapidement adopté par une communauté de développeurs pour lui ajouter davantage de fonctionnalités. L'intégration du noyau Linux avec le SE libre GNU donna ainsi naissance au SE libre GNU/Linux. Plusieurs sociétés et individus se mirent alors à construire des distributions GNU/Linux en intégrant diverses applications à un tronc commun constitué d'une version du noyau Linux et des outils logiciels du projet GNU. C'est ainsi que sont nées les distributions GNU/Linux comme Slackware, Red Hat, Debian, Gentoo, pour les plus anciennes et qui existent encore de nos jours, et d'autres plus récentes comme Mandriva, Fedora, Ubuntu, etc.

Des caractéristiques intéressantes pour les utilisateurs finaux

Le système d'exploitation GNU/Linux possède les caractéristiques du SE Unix : il est multi-tâches, multi-utilisateurs et, en particulier, tous les utilisateurs ajoutés au système ne possèdent pas les droits d'administration du système. Seul le « super-utilisateur », appelé communément *root*, possède ce droit d'administration. Un tel système d'exploitation satisfait donc déjà à l'une des règles importantes de sécurité de ne pas travailler avec un compte ayant pouvoir d'administration. Par ailleurs, le système de fichiers sous GNU/Linux étant différemment conçu que celui de Microsoft Windows, il s'en suit que les programmes malveillants conçus pour attaquer les systèmes d'exploitation Windows sont inopérants sous GNU/Linux. Cette dernière propriété fait du système GNU/Linux le meilleur logiciel anti-virus à l'heure actuelle, en particulier pour des pays comme le Vietnam, pour les raisons suivantes :

- Pour une personne débutante et pas encore habituée à un système d'exploitation donné, la courbe d'apprentissage d'une distribution GNU/Linux orientée vers la bureautique comme Ubuntu ne paraît pas plus compliquée, en absolu, que pour le système d'exploitation MS Windows.
- Les logiciels libres permettant généralement une facile traduction, en particulier par la communauté des utilisateurs, il s'en suit que des distributions GNU/Linux comme Ubuntu sont disponibles sous de nombreux langages dont le vietnamien, ce qui est un atout majeur pour une meilleure maîtrise du logiciel et du SE dans un pays où le niveau de maîtrise des langues étrangères, comme l'anglais ou le français, est faible.
- Les distributions GNU/Linux orientées bureautique comprennent un ensemble d'applications bureautique qui conviennent aux besoins de base d'un poste de travail bureautique : traitement de texte évolué, courrier électronique, navigation internet, traitement des images, etc. Elles sont distribuées avec une licence libre dont le coût est gratuit. De ce fait les distributions GNU/Linux répondent parfaitement aux besoins des utilisateurs des pays en voie de développement comme le Vietnam qui peuvent alors utiliser des logiciels sûrs et performants en toute légalité et éviter les coûts souvent prohibitifs des logiciels commerciaux non libres.

Avec de tels avantages, comment se fait-il que le système GNU/Linux ne soit-il pas davantage répandu ?

Le Vietnam, comme pour la majorité des pays du monde, « importe » les technologies de l'information pour les utiliser. Sur le plan historique, le système GNU/Linux est arrivé sur le marché après le système MS-DOS et MS-Windows qui avaient alors une bonne main mise sur le marché des SE de l'ordinateur individuel. Les logiciels commerciaux non libres introduits au Vietnam étant généralement piratés, les utilisateurs locaux restent encore faiblement sensibilisés aux problèmes juridiques liés aux licences d'utilisation des logiciels. Les logiciels commerciaux étant disponibles sur le marché pour un prix dérisoire, il n'existe donc pas de motivation pour rompre les habitudes et se diriger vers les logiciels libres. De plus, tous les supports de formation et la littérature informatique sont basés sur les logiciels commerciaux non libres dont l'usage est répandu au Vietnam. Il s'en suit que trouver un support local, en vietnamien, pour apprendre à utiliser les logiciels libres est encore difficile, faute de marché conséquent. Les vendeurs d'ordinateurs sont le plus souvent ignorants de l'existence d'autres alternatives au système d'exploitation MS-Windows et installent d'emblée tout un jeu d'applications avec le système MS-Windows sur tout nouvel ordinateur vendu. Il y a là une sorte de cercle vicieux qui est un obstacle à la propagation de l'utilisation des logiciels libres, dont le système d'exploitation GNU/Linux, qu'il faut rompre. C'est une chose faisable car de nombreux exemples de migration du système d'exploitation MS-Windows vers GNU-Linux existent de par le monde et ont été documentés. Par exemple, il y a le cas célèbre de la gendarmerie française qui a déjà migré plus de 10.000 postes vers la distribution GNU/Linux Ubuntu en 2009 et qui compte faire une migration complète de ses 70.000 postes à l'horizon 2015 [11]. Au sein de l'Agence universitaire de la Francophonie même, un processus de migration similaire est sur le point d'être complètement achevé, ce qui représente près de 2.500 postes de travail répartis sur 66 implantations à travers le monde.

Une telle migration, de MS-Windows vers GNU/Linux, peut tout à fait être envisagée au Vietnam dès qu'elle est bien préparée et après avoir réuni toutes les conditions nécessaires. Le Vietnam, depuis sa candidature comme membre de l'Organisation mondiale du commerce a du s'engager à faire respecter les droits de la propriété intellectuelle, dont ceux des logiciels. Plusieurs directives ministérielles récemment publiées encouragent les organismes gouvernementaux à utiliser les logiciels libres dont une liste a été rendue publique. Par ailleurs, une communauté d'utilisateurs des logiciels libres, dont GNU/Linux, a commencé de s'organiser dans les grandes villes comme Hanoi et Hô Chi Minh-Ville pour promouvoir l'utilisation des logiciels libres. Il devient clair que petit à petit l'oiseau est en train de faire son nid et que vouloir aujourd'hui utiliser un poste informatique en toute sécurité, sans plus avoir à besoin de se soucier des virus et autres programmes malveillants, ni à se soucier des problèmes de renouvellement de licences, est devenue une chose possible avec le niveau de maturité atteint par les logiciels libres, en particulier les distributions GNU/Linux. Un autre aspect non moins important est la liberté de choix que confèrent les logiciels libres par rapport à un choix unique, celui de MS-Windows, comme c'est le cas en pratique, à l'heure actuelle au Vietnam.

Donc, pour conclure cet exposé, j'aimerais paraphraser feu le président Hô Chi Minh pour qui « Rien n'est plus précieux que l'indépendance et la liberté », ce que justement confèrent les logiciels libres dans le monde des technologies de l'information

Références

- [1] “Bonne performance d’Apple et Linux en 2008 face à la déception Vista,” *AT Internet Institute*, Jan. 2009 [<http://www.atinternet-institute.com/fr-fr/equipement-internaute/systemes-d-exploitation-decembre-2008/index-1-1-7-155.html>].

- [2] “+37% de Linuxiens en un an ! - fgv6.net,” *fgv6.net*, Jun. 2008 [<http://www.fgv6.net/37-de-Linuxiens-en-un-an.html>].
- [3] “Insécurité du système d'information - Wikipédia,” *Wikipédia*, Sep. 2009 [http://fr.wikipedia.org/wiki/Insécurité_du_système_d'information].
- [4] “Tội phạm công nghệ cao ngày càng tinh vi - Công nghệ thông tin - NLĐO,” *Người Lao Động online*, Mar. 2009 [<http://www.nld.com.vn/2009032908135641P0C1039/toi-pham-cong-nghe-cao-ngay-cang-tinh-vi.htm>].
- [5] “Có 3.594 dòng virus máy tính mới xuất hiện tại Việt Nam trong tháng 9 - Công nghệ thông tin - NLĐO,” Oct. 2008 [<http://www.nld.com.vn/241326P0C1039/co-3594-dong-virus-may-tinh-moi-xuat-hien-tai-viet-nam-trong-thang-9.htm>].
- [6] “Việt Nam: tổn thất 327 tỷ VNĐ mỗi tháng vì virus - Tin tức - Sự kiện - Xã hội thông tin online,” *Xã Hội Thông Tin*, Mai. 2009 [<http://www.xahoihongtin.com.vn/20090513032620426p0c206/viet-nam-ton-that-327-ty-vnd-moi-thang-vi-virus.htm>].
- [7] “Survival Time | SANS Internet Storm Center; Cooperative Network Security Community - Internet Security,” *SANS Internet Storm Center* [<http://isc.sans.org/survivaltime.html>].
- [8] “Asia Marketing Research, Internet Usage, Population Statistics and Information,” *Internet World Stats: Usage and Population Statistics* [<http://www.internetworldstats.com/asia.htm#vn>].
- [9] “GNU Operating System,” *gnu.org* [<http://www.gnu.org/>].
- [10] “GNU General Public License,” *gnu.org*, Jun. 2009 [<http://www.gnu.org/licenses/gpl.html>].
- [11] P. Ryan, “French police: we saved millions of euros by adopting Ubuntu,” Mar. 2009 [<http://arstechnica.com/open-source/news/2009/03/french-police-saves-millions-of-euros-by-adopting-ubuntu.ars>].