L'imprimante Unique : Un pas vers les impressions totalement sécurisées

Eric WIES
Service Informatique – UFR MIM
Université Paul VERLAINE
Ile du Saulcy, 57 045 METZ CEDEX 1

Résumé

Malgré les efforts des constructeurs, et l'amélioration des protocoles, l'impression reste l'élément oublié de la sécurité des documents. Après avoir passé en revue l'impression réseau et les moyens de protéger un document lors de sa transmission vers l'imprimante, nous proposerons une architecture type pour la mise en place d'un service d'impression sécurisé.

Notre travail se décomposera en deux phases. Dans un premier temps, nous allons créer un périphérique unique – l'imprimante unique - qui recevra l'ensemble des impressions et les répartira dans un réseau dédié. Dans un second temps, ce périphérique proposera une liaison chiffrée avec les postes demandeurs d'impressions évitant ainsi les attaques de type « homme du milieu ».

En isolant et cachant les identités réelles des imprimantes, et en réalisant une transmission chiffrée nous atteindrons plusieurs objectifs. D'une part de rendre le poste client indépendant de son imprimante et donc gérer son remplacement à la volée. D'autre part protéger l'impression du document de bout en bout. Enfin, notre solution nous permet de sécuriser un parc d'impression sans changer aucune imprimante.

Mots clefs

Impression, protection de document, liaison chiffrée, disponibilité

1 De l'imprimante réseau à la sécurité de l'impression

On sait depuis longtemps protéger un document écrit. De sa création à sa destruction, on a su mettre en place des procédures strictes. Cependant avec l'explosion des périphériques d'impression, voire des périphériques combinés (fax, scanner, imprimante) se pose le problème de la sécurité de l'impression. En effet, comment protéger un document qui va parcourir un réseau puis sortir sur une imprimante parfois éloigné du demandeur de l'impression ? Longtemps considérée comme le parent pauvre de la sécurité des documents, les fuites d'informations liées à l'impression commencent à inquiéter les entreprises [1]. Les institutions [2] comme les constructeurs [3] se sont penchés sur ce problème avec des approches différentes. Après avoir fait le point sur l'impression réseau et sur la sécurité de l'impression, nous proposerons une méthode permettant de sécuriser tout le processus d'impression en conservant nos périphériques actuels.

1.1 Historique de l'impression réseau

Le partage du périphérique d'impression est devenu une nécessité dès que nos machines se sont trouvées interconnectées [4]. En effet, plutôt que de dupliquer les capacités d'impression on a préféré les partager surtout si les capacités diffèrent d'une machine à l'autre (impression recto-verso, jet d'encre couleur, laser couleur, impression dans d'autres formats). La première technique qui vient à l'esprit est d'utiliser un système de partage de ressources, permettant de partager nos capacités d'impression vers d'autres machines (lpr, cups, samba, netbios, apple talk). Puis les imprimantes sont devenues, grâce à des composants internes ou externes[1], des périphériques réseaux[2] à part entière. Nous allons étudier les deux cas, bien que le premier devienne de plus en plus obsolète.

[1]Ces boîtiers sont souvent appelés « serveur d'impression », ici on se contentera de l'appellation « boîtier externe » pour ne pas engendrer de confusion avec un serveur d'impression qui a la charge de plusieurs imprimantes.

[2]On préféra le terme « périphérique réseau » à celui de « périphérique IP », bien que les réseaux IP soient majoritaires dans nos universités, les capacités des périphériques dépassent largement le protocole IP. On devra s'en souvenir si l'on doit protéger l'impression dans un milieu sensible.

Le partage d'imprimante est tellement courant qu'il suffit d'installer une machine avec une imprimante sous Windows (netbios) ou sous Linux (cups) pour que celle-ci soit automatiquement utilisable par les autres utilisateurs. On se retrouve d'ailleurs parfois dans des situations ubuesques où on est amené à partager une imprimante qui est déjà partagée par un autre système. On se retrouve alors avec une liste impressionnante d'imprimantes alors que les propriétaires de celles-ci n'ont pas conscience qu'elles soient accessibles à autant de monde. De même, on retrouve des imprimantes partagées alors que celles-ci possèdent des listes de contrôles d'accès strictes. Outre les problèmes de sécurité et de confidentialité que cela suppose, ce type de configuration génère un flux réseau important. En effet, les machines annoncent leur capacité de partage à tout le réseau de façon systématique et répétitive (toutes les 30 secondes dans un réseau samba/netbios ou cups). De plus, le flux d'impression traverse le réseau dans un sens (jusqu'au poste qui partage sa capacité d'impression) puis repart dans l'autre sens (jusqu'au périphérique d'impression).

Un des autres inconvénients du partage à partir d'un poste de travail est que celui-ci reçoit toute la charge d'impression. De ce fait il en garde le contrôle, ce qui peut être vu comme un avantage ou un inconvénient suivant la qualité (restreint, secret, confidentiel) des impressions effectuées et du volume de données traitées par le poste pour réaliser ses impressions. Enfin, il ne faut pas oublier que le poste qui partage l'impression doit toujours être allumé, ce qui exclut d'utiliser les systèmes d'économie d'énergie comme l'hibernation, la mise en veille prolongée ainsi que des ordinateurs portables.

Le partage d'imprimante reste la solution des petits réseaux qui n'ont que des imprimantes USB. Cependant elle n'est pas adaptée à notre milieu universitaire où le partage de la ressource d'impression est la raison même d'exister de celle-ci. Bien sûr il reste quelques périphériques d'impression spécifiques (grands formats, papiers spéciaux, couleurs spécifiques) que l'on ne souhaite pas partager (pour une redistribution des coûts par exemple) ou du moins pas de façon simple. Nous exclurons ces périphériques de notre étude.

Même pour les imprimantes qui possèdent une capacité réseau propre [5] (qu'elles soient internes ou externes) nous avons deux possibilités de gérer les impressions. Nous pouvons utiliser chaque imprimante comme un périphérique d'impression distinct ou centraliser toutes les impressions sur un serveur qui communiquera avec les imprimantes. Nous allons détailler ces deux cas et tenter de les comparer.

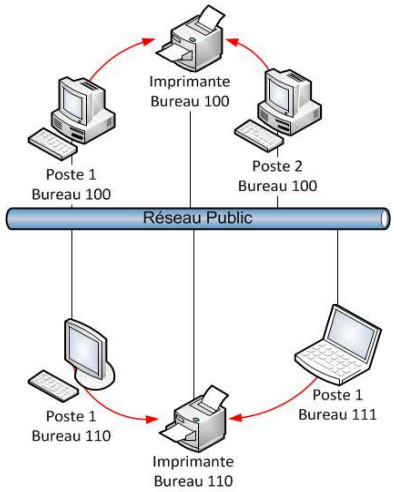

Figure 1 - L'impression réseau

- Impression réseau avec des imprimantes réseaux. (6) L'impression utilisant des périphériques d'impression réseaux est la solution la plus simple [7] (Figure 1 - L'impression réseau).Pour partager une imprimante dans un bureau ou laboratoire de recherche, il suffit d'installer le pilote et d'indiquer l'adresse réseau (parfois trouvée automatiquement par le programme d'installation [8]) de l'imprimante pour disposer immédiatement de la ressource d'impression [9].

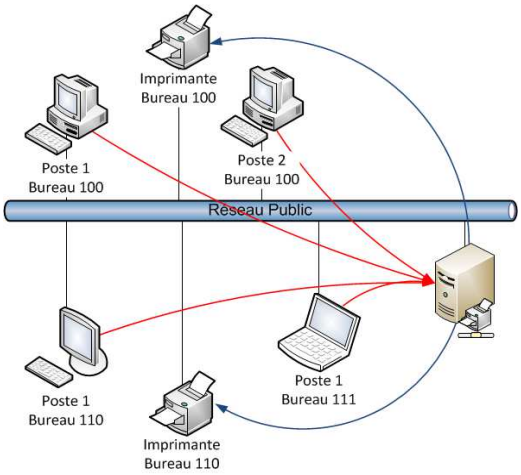

Figure 2 - L'impression réseau avec un serveur d'impression

- Impression réseau avec un serveur d'impression. L'utilisation d'un serveur d'impression (Figure 2 - L'impression réseau avec un serveur d'impression) apporte de nombreux avantages. L'un des plus importants est le contrôle central de la file d'impression. Ce contrôle devient fondamental quand il y un grand nombre de clients utilisant la même imprimante. Sans ce contrôle, il faudrait accéder à chaque client pour annuler une impression [10]. Mais on peut aussi citer la création d'un *pool* d'imprimantes et la possibilité d'identifier les utilisateurs de la ressource d'impression. Dans notre problématique on retiendra surtout que le serveur d'impression peut délivrer les pilotes des périphériques à la demande du client. Cette fonctionnalité permet à l'administrateur de préparer tous les pilotes à l'avance et simplifie grandement l'installation d'un nouveau client au serveur d'impression. Une des phases de notre problème semble donc réglée. En effet si le client nécessite toujours l'installation du bon pilote, celui-ci est toujours disponible car il est délivré par le serveur (sous réserve que l'administrateur ait mis à disposition tous les pilotes de toutes les imprimantes concernées). De plus, le serveur ne communiquant que le nom de partage de l'imprimante, le client se trouve indépendant de l'adresse réseau de la ressource d'impression.

Cependant cette technique a ses limites. En effet le changement d'une imprimante impose la modification du pilote sur le serveur et le cas échéant un passage sur chaque client pour redéfinir l'imprimante par défaut.

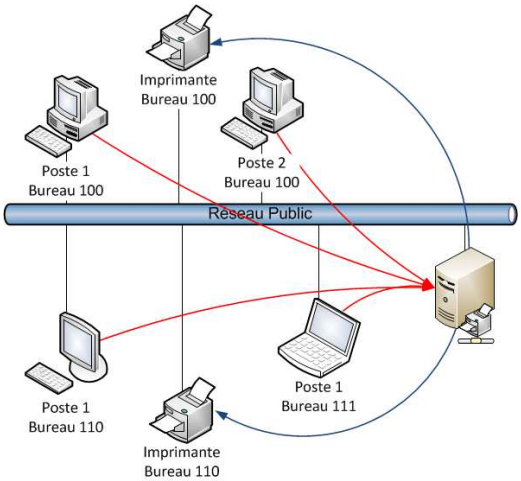

Figure 3 - Utilisation d'un réseau d'impression

Dans nos parcs universitaires, l'impression réseau avec un serveur d'impression semble la plus adapté [11]. Nous pouvons même placer les imprimantes dans un réseau séparé, plus pour un souci de libération d'adresse IP que de sécurité (Figure 3 - Utilisation d'un réseau d'impression). Cependant pour optimiser nos installations, nous utilisons des systèmes d'installations massives qui nous permettent d'installer un ensemble de machines depuis une machine modèle.

Pour installer massivement nos parcs nous utilisons depuis longtemps des outils capables [12] de répliquer une machine modèle vers un ensemble de machines semblables. Il existe différents systèmes pour « cloner » une machine, du plus basique (démontage physique du disque) au plus évolué (déploiement automatique de l'image). Dans la problématique qui nous intéresse le but n'est pas tant d'avoir un système autonome opérationnel rapidement, mais un système « prêt à imprimer ».

Nous avons vu qu'il existe deux grandes familles d'impression réseau. La première est d'utiliser directement l'imprimante comme périphérique réseau. Si toutes les machines installées massivement (i.e. clonées) utilisent la même imprimante, il suffit de l'avoir installée dans la machine modèle. Cependant ce cas n'est pas le cas général, il s'applique assez bien pour une salle de travaux pratiques, mais très mal quand il s'agit d'installer des postes administratifs ou d'enseignants chercheurs. Nous avons perdu donc une grande partie du bénéfice de la machine modèle car toutes les machines doivent être reconfigurées avec la bonne ressource d'impression.

La seconde famille, impression à l'aide d'un serveur d'impression, va se montrer beaucoup plus adaptée à l'installation massive. En effet, le serveur d'impression étant le même pour tout le monde, et disposant des pilotes des imprimantes, il suffit d'installer la bonne imprimante parmi celles proposées sur le serveur. Bien qu'en apparence plus simple, elle nécessite de passer sur chaque poste pour « installer » l'imprimante voulue.

Nous définissons ici une technique qui va nous permettre de nous affranchir de cette étape. En effet, le poste imprimera toujours sur la même imprimante, et dans un second temps toujours avec le même pilote. Nous pourrons donc cloner une machine puis la placer dans son contexte. L'activation de ses ressources d'impression sera automatiquement validée par notre périphérique et ne nécessitera pas de configuration a posteriori sur le poste de travail.

1.2 La sécurité de l'impression

La sécurité de l'impression n'a été prise en compte que très récemment. Il y a au moins trois grands problèmes à résoudre :

- Le premier est l'accès au document papier, car l'impression est souvent réalisée dans une pièce commune et donc le document pourra être lu, voire dupliqué, avant qu'il soit récupéré par son demandeur (quand il n'est pas subtilisé tout simplement – combien de personnes se plaignent, après avoir lancé une impression mais que le document n'est jamais sorti).

- Le second est la communication avec l'imprimante. La communication peut elle-même être décomposée en deux parties, la transmission du document à l'imprimante et l'administration de l'imprimante.

- Le troisième est le stockage même du document dans l'imprimante. En effet, une imprimante est devenue un système matériel – logiciel à part entière disposant de sa mémoire de masse. Le problème est d'autant plus grave que nous disposons de périphériques loués. Nous ne traiterons pas ce problème car il doit être traité par le constructeur de l'imprimante, et des solutions de chiffrement de disque et d'effacement de sécurité des documents commencent à apparaître sur ces imprimantes. L'utilisateur étant sensibilisé à ce problème, il évitera de faire réaliser des travaux de nature sensible et confidentielle par ce type de machine.

L'accès au document est devenu l'argument commercial numéro 1 des constructeurs d'imprimantes. Ils proposent tous au moins une solution pour attendre que le demandeur d'impression se présente devant l'imprimante pour sortir le document attendu (digicode, carte à puce, carte sans contact). Cette protection bien qu'élégante, n'intervient qu'en bout d'impression. En effet, le document a déjà parcouru le réseau et a pu être intercepté pendant ce transfert. Elle a quand même le mérite de limiter la diffusion du document papier, protégeant ainsi la circulation des documents.

La plupart des protocoles diffusent l'impression en clair sur le réseau. Ils sont donc sensibles à toutes les usurpations d'adresses et toute déviation d'un flux réseau pour réaliser l'écoute des documents. Il n'y a que le protocole IPP qui peut permettre un chiffrage

des données (quand il est encapsulé dans un protocole SSL/TLS), mais cette sécurité n'est que trop rarement utilisée (car le client et le périphérique doivent supporter cette surcouche).

Il ne faut pas non plus oublier tous les protocoles de gestion de l'imprimante (telnet et http en général). Ces protocoles ne sont pas chiffrés et permettent un grand contrôle du périphérique d'impression. On peut modifier les caractéristiques réseaux et par exemple modifier son adresse ip en vue de l'utiliser pour y placer un autre périphérique mais aussi réimprimer le dernier document.

1.3 Comment sécuriser l'impression ?

Nous avons vu que même si, dans le meilleur des cas, le document ne sort pas de l'imprimante, son parcours vers celle-ci est des plus dangereux. Nous allons proposer une méthode permettant de rendre ce parcours un peu plus sécurisé et un peu plus lisible pour l'administrateur réseau.

2 L'imprimante Unique

Nous allons décomposer notre technique en deux phases. Dans un premier temps nous allons faire imprimer tous les postes vers une seule et même adresse sur le réseau (une unique cible d'impression). On rendra alors le poste indépendant de l'adresse de la ressource d'impression. Dans un second temps, tous les postes imprimeront avec le même protocole (postcript), ce qui le rendra indépendant du pilote du constructeur.

2.1 Cible unique d'impression

Pour réaliser la cible unique d'impression nous allons simplement installer et configurer un redirecteur de paquets sur notre périphérique « imprimante unique » (Figure 4 - L'imprimante Unique). Le redirecteur décidera vers quelle imprimante les paquets d'impressions sont dirigés. Pour construire le redirecteur, nous utiliserons simplement des règles de pare-feu (dans notre cas netfilter) qui va utiliser la réécriture des paquets pour translater un paquet d'un réseau public vers un réseau privé. Nous avons deux choix pour construire ce redirecteur. Le premier est manuel en ajoutant les règles au fur à mesure qu'un poste ou qu'une nouvelle imprimante est ajoutée dans le système. Une seconde approche est de définir un fichier de configuration puis de générer automatiquement les règles de redirection.

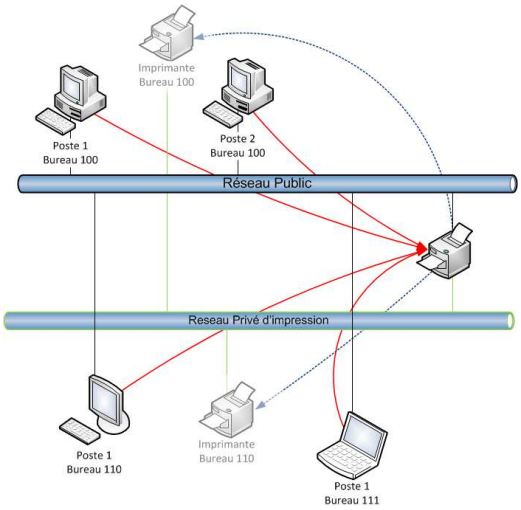

Figure 4 - L'imprimante Unique

L'écriture d'une redirection de façon manuelle ou automatique impose de connaître exactement le protocole de communication de l'imprimante concernée (dans la pratique il nous suffit de connaître le port, car toutes les imprimantes actuelles communiquent avec le protocole TCP, on peut rencontrer le protocole IPP mais c'est une surcouche de tcp). Parmi ces ports on peut trouver les ports 515 (lpr), 80 (http), 443 (https), 631 (cups), 9100 (ipp [13]). Heureusement on peut trouver ces ports facilement en inspectant la configuration d'un poste dans son installation de base (paramètres d'impressions) et dans le doute, nous pourrions facilement rediriger tous ces ports.

Nous obtenons donc un périphérique capable de concentrer toutes les demandes d'impressions et de les rediriger vers la bonne cible. Cette redirection apporte de nombreux avantages. Tout d'abord elle ne ralentit pas le flux d'impression, le client, comme l'imprimante destinataires sont toujours dans le même réseau virtuel (l'imprimante unique est venue s'interposer entre les deux, se faisant passer pour le client à l'imprimante et pour l'imprimante au client). Ensuite, l'ensemble des périphériques d'impression possède son propre réseau et ne vient plus polluer nos réseaux publics. Enfin le réseau privé d'impression est caché à l'ensemble de nos utilisateurs. Ceci dit, notre périphérique reste malléable et adaptable à tout moment, puisqu'il peut associer de nouveaux clients, voire de nouvelles imprimantes sans modifier l'adressage ip.

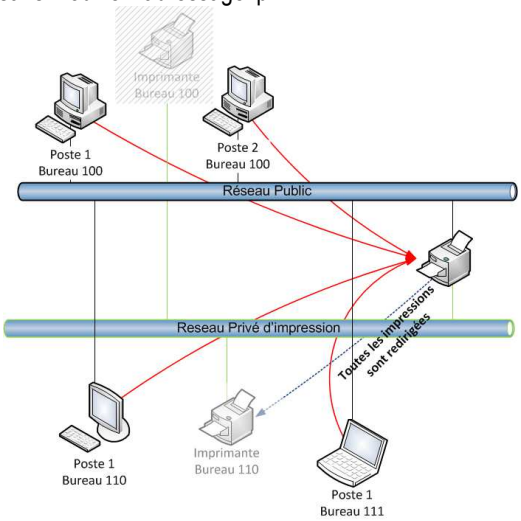

Figure 5 - Changement d'imprimante à la volée

Il nous reste une étape à franchir pour permettre l'échange d'imprimante à la volée sans aucune intervention sur les postes clients. En effet le changement de périphérique physique d'impression s'accompagne souvent du changement de pilote d'impression, nous allons donner quelques pistes pour utiliser un protocole unique d'impression.

2.2 Protocole unique d'impression

L'utilisation d'un protocole unique est basée sur le fait que la plupart des périphériques d'impression utilisent soit le protocole postscript1 (Adobe), soit le protocole PCL2 (Hewlett-Packard [14]). On est donc tenté d'installer l'un ou l'autre de ces protocoles (ou les deux) pour contrôler toutes nos imprimantes. On remarquera que la plupart des imprimantes compatibles PCL, sont aussi compatibles postscript (l'inverse étant rarement vrai). La tentation est donc grande de ne s'occuper que du protocole postscript mais nous devons alors perdre des fonctions avancées de nos périphériques comme le recto-verso. Nous avons posé comme postulat de ne perdre aucune fonctionnalité (nos utilisateurs ne doivent pas remarquer l'utilisation de l'imprimante unique). Nous allons donc choisir au mieux le pilote correspondant le plus aux besoins de l'utilisateur.

2.3 Plusieurs protocoles et plusieurs imprimantes ?

Le cas des imprimantes multiples (i.e. un poste doit pouvoir imprimer sur plusieurs imprimantes) n'est pas un problème complexe pour notre solution. En effet, il suffit de changer le port par défaut dans la configuration de la seconde imprimante (en conservant toujours la même adresse réseau, dans la pratique nous ajoutons 1 au port précédent utilisé) pour que l'imprimante unique dirige l'impression vers le second périphérique. Nous déclarons même systématiquement deux imprimantes. Quand l'imprimante unique ne décèle qu'une seule imprimante physique elle redirige simplement ces deux flux vers la même imprimante. Bien entendu nous ne sommes pas limités à deux imprimantes et notre système est extensible à un grand nombre d'imprimantes par poste.

Nous avons deux grandes familles de problèmes pour les protocoles multiples. :

- La première est le fait d'utiliser plusieurs protocoles pour piloter la même imprimante (utiliser à la fois postscript et pcl). La seconde est d'utiliser un protocole spécifique pour un périphérique donné. Le premier cas ne pose pas de grandes difficultés. En effet, on peut créer autant d'imprimantes que nécessaires, chacune imprimera sur le même périphérique

physique mais avec un protocole différent. L'utilisation de protocoles spécifiques est un peu plus complexe. Parfois on ne pourra se passer d'installer le pilote propre à l'imprimante sur certains postes. En effet certaines imprimantes exotiques ne comprennent que leur propre protocole et de ce fait ne pourront pas entrer dans la seconde phase de notre solution. Ceci nous impose une limitation quand au remplacement du périphérique d'impression à la volée mais cette problématique reste heureusement marginale.

- Il nous reste le cas des protocoles qui ne sont pas directement des protocoles d'impression, mais plutôt des protocoles de contrôle [15] et de surveillance des périphériques d'impression (snmp ou web). Bien que l'on puisse régler ce problème facilement quand il faut remplacer une imprimante, on se heurte à des difficultés quand un poste utilise plusieurs imprimantes. En effet, bien que l'on puisse déplacer l'accès au site web embarqué dans le périphérique d'impression[3], on ne peut pas modifier le port interrogation snmp[4] facilement. Nous avons donc choisi dans notre implémentation de nous occuper uniquement des protocoles d'impression.

3 Sécurisation des impressions

La problématique de la sécurisation des documents est double. Il nous faut d'abord nous assurer que le périphérique d'impression n'a pas été usurpé. Puis, dans un second temps, chiffrer toute demande d'impression vers ce périphérique. Nous allons utiliser le protocole SSL qui répond aux deux problématiques simultanément.

3.1 Chiffrer les documents

Le chiffrement des documents va s'obtenir en insérant les documents dans un tunnel chiffré (Figure 6 - Chiffrement des communications). La configuration locale (sur le poste) de l'imprimante va définir comme cible d'impression la boucle locale (localhost, 127.0.0.1). De là les informations seront chiffrées localement et transmisent à l'imprimante Unique qui déchiffrera et répartira les flux d'impressions.

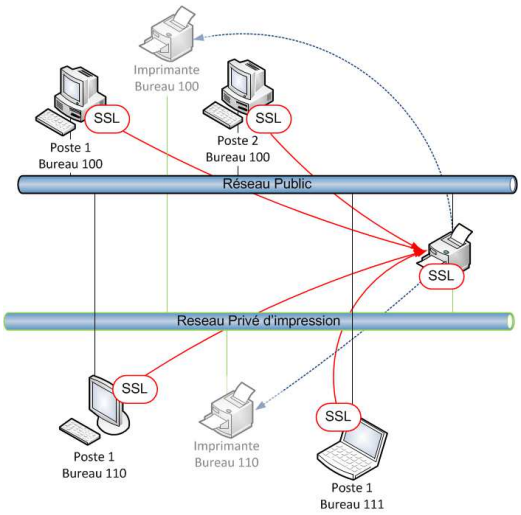

Figure 6 - Chiffrement des communications

Nous avons réalisé nos tests de faisabilité en utilisant simplement un tunnel ssh. Ceci nous permet donc de faire transiter dans un tunnel ssh (putty sous windows et openssh sous Unix/Mac OS X) une communication attendue sur l'adresse locale du poste (localhost) et redirigée vers l'imprimante unique. Cette solution répond pleinement au problème de chiffrage des documents et d'authentification de l'imprimante unique mais n'est pas très élégante, tant pour l'utilisateur (qui doit lancer son tunnel avant chaque impression ou le laisser ouvert en permanence) que pour la charge réseau (qui voit un flux ssl constant, même quand aucun document n'est imprimé).

[3]On pourrait le déplacer sur le port 80 vers le port 8080 par exemple, et créer un marque page dans le navigateur du poste.

[4]La problématique vient du protocole snmp lui même, le port 161 est souvent placé directement dans les programmes de status d'impression

Pour éviter les désagréments du tunnel ssh activé en permanence, nous avons développé une petite application client/ serveur qui ne monte la liaison sécurisé qu'en présence de documents à imprimer. Pour cela, l'application écoute en permanence le port d'impression sur l'adresse de la boucle locale. Si un document transite, la liaison s'active et se désactive d'elle-même à la fin de l'impression. Nous utilisons pour cela les drapeaux TCP/IP du flux d'impression qui signalent la fin d'une transmission de données.

3.2 Protection de l'imprimante unique

L'imprimante unique repose sur le fait que la fausse imprimante (une machine standard équipée de deux cartes réseaux) soit capable d'identifier la source et la destination de l'impression pour pouvoir faire un mappage réseau entre le réseau public et le réseau privé réservé aux imprimantes. Cela impose souvent d'amener ces deux réseaux dans chaque bureau.Nous devons donc penser à la charge supplémentaire d'administration des VLAN et des ACL de ces différents commutateurs.

Les attaques sur le réseau d'impression lui-même sont encore possibles. En effet, le rendre invisible pour l'utilisateur ne le protège pas pour autant. Pour éviter ces désagréments, il convient d'utiliser un outil permettant de détecter l'usurpation d'adresses IP et d'adresses MAC (on va en fait détecter le déplacement physique d'une imprimante d'un bureau dans un autre).

L'imprimante Unique devenant un point de faiblesse majeur (la perte de cette machine entraîne la perte de toutes les capacités d'impression), nous avons créé un double sur le réseau. Le double est chargé de veiller à l'existence de l'Imprimante Unique et de prendre sa place le cas échéant (en changeant dynamiquement son adresse ip). Les composants logiciels de l'Imprimante Unique ne nécessitant pas de grandes ressources, n'importe quelle machine ayant connaissance des réseaux publics et d'impression peut facilement prendre cette fonction.

4 Conclusion

Nous avons construit un système d'impression sécurisé totalement transparent pour l'utilisateur. Nous pouvons continuer d'utiliser tous nos périphériques d'impression – même les plus vulnérables - et la sécurité n'est pas venue au détriment d'autres fonctionnalités. Notre solution ne génère pas de « surcoût » de sécurité, mais nécessite de bien préparer ses réseaux. Nous travaillons actuellement sur une interface intuitive, permettant de contrôler l'imprimante unique de manière graphique (gestion des postes, des imprimantes et des liaisons entre ceux-ci).

5 Remerciements

Nous tenons ici à remercier pour leur confiance, l'ensemble des personnels et la direction de l'Unité de Formation et de Recherche en Mathématique Informatique Mécanique, Automatique (UFR MIM) de l'Université Paul VERLAINE - METZ, qui nous a laissée toute liberté pour réorganiser l'impression à l'échelle d'une UFR.

6 Bibliographie

[1] Guestault, François. *L'impression sécurisée et son rôle dans la stratégie de sécurité de l'entreprise.* [Spywolrd Actu]. [En ligne] 26 2 2008. http://www.spyworld-actu.com/spip.php?article7081.

[2] ENISA. *Impression sécurisée*. s.l.: European Network And Information Security Agency, 2008. 978-92-9204-009-3.

[3] Brancier, Christiène. http://pro.01net.com/editorial/339836/limpression-securisee-un-marche-a-attaque . 01net pro. [En ligne] 29 1 2007.

[4] STORM, David. *Networking Survival Guide*. New York, NY, USA : McGraw-Hill, Inc, 2001.

[5] Todd RADEMACHER, Matthew GAST. *Network printing*. Sebastopol, CA, USA : O'Reilly & Associates, Inc., 2000.

[6] R. HERRIOT, R. DEBRY, S. ISAACSON, P. POWELL. *Internet Printing Protocol/1.1 : Model and Semantics*. 2000, RFC Editor, http://www.ietf.org/rfc/rfc2910.txt

[7] WRIGHT, F. RFC2567: D*esign Goals for an Internet Printing Protocol. United States* : RFC Editor, 1999. http://www.rfc-editor.org/rfc/rfc2567.txt

[8] FINKE, Jon.. *Automating Printing Configuration Source*. San Diego, California : s.n., 1994. Proceedings of the 8th USENIX conference on System administration. pp. 175-184.

[9] WRIGHT, F.D. *Requirements and design goals for an Internet printing protocol.* ACM Volume 6, Issue 4. [1]December 1998.

[10] WU, Albert K. W. *A poor man's access to laser printing facilities.* Volume 25, Issue 3, September 1995. ACM SIGUCCS Newsletter. pp. 16-20.

[11] Scott HANSELMAN, David PRZYBYLA. *Printing in today's academic labs: not exactly what Gutenberg had in mind.* 2005, Proceedings of the 33rd annual ACM SIGUCCS conference on User services, pp. 105-108.

[12] Pascal AUBRY, Katy SANTERRE. *Clonage et déploiement de PC avec REMBO*. 2003. Congrès JRES. p. Sessions posters.

[13] MANROS, Carl-Uno. *The birth of the Internet printing protocol (IPP).* New York, NY, USA : s.n., Volume 6 , Issue 4, 1998. ACM. pp. 135-139.

[14] PADWICK, Gordon. *Hewlett-Packard's guide to color printing techniques.* New York, NY, USA : Random House Inc, 1995.

[15] C. KUGLER, H. LEWIS, T. HASTING. *RFC3239: Internet Printing Protocol (IPP): Requirements for Job, Printer, and Device Administrative Operations.* 2002, RFC Editor, http://www.rfc-editor.org/rfc/rfc2567.txt

[16] SHEPPARD, Rob. *Epson Complete Guide to Digital Printing.* s.l. : Sterling Publishing Company, Incorporated, 2003.

[17] Guillem BORGUESI, Christophe BOCCHECIAMPE. *Réinstallation de postes clients avec PXE et Partimage.* 2007. Congrès JRES. p. Article 33, http://2007.jres.org/planning/paper7451.html?pid=33