Groupe de travail Réseau
Request for Comments : 2148
BCP : 15
Catégorie : Bonnes pratiques actuelles

H. Alvestrand, UNINETT
P. Jurg, SURFnet
septembre 1997
Traduction Claude Brière de L'Isle

Déploiement du service de pages blanches de l'Internet

Statut de ce mémoire
Le présent document spécifie les bonnes pratiques actuelles de l'Internet pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. La distribution de ce mémoire n'est soumise à aucune restriction.

1. Résumé et recommandations

Le présent document fait les recommandations suivantes aux organisations de l'Internet :

1. Une organisation DEVRAIT publier ses informations d'adresses de messagerie électronique et autres adresses publiques sur les utilisateurs de l'Internet au sein de son site.

2. La plupart des pays ont des lois concernant la publication des informations touchant les personnes. Au delà et à côté de cela, les organisation DEVRAIENT suivre les recommandations de [1].

3. La façon préférée actuellement pour la publication des informations est d'utiliser X.500 comme structure de données et schéma de dénomination (défini dans [4] et exposé dans [3], mais certains pays utilisent un raffinement national, comme [15] pour les USA). L'organisation PEUT aussi les publier en utilisant des structures de données supplémentaires comme avec whois++.

4. L'organisation DEVRAIT rendre les informations publiées disponibles aux clients LDAP, en permettant que les serveurs LDAP accèdent à leurs données.

5. L'organisation NE DEVRAIT PAS tenter de facturer le simple accès aux données.

De plus, il fait les recommandations suivantes pour toutes les diverses autres parties :

1. Les fournisseurs de messagerie électronique DEVRAIENT inclure la fonction de recherche LDAP dans leurs produits, soit comme fonction incorporée, soit en fournissant des facilités de traduction.

2. Les fournisseurs d'accès Internet DEVRAIENT aider les plus petites organisations à suivre ces recommandations, soit en fournissant des services d'hébergement de leurs données, en les aidant à trouver d'autres partenaires pour le faire, soit en les aidant à mettre leur propre service en ligne.

3. Toutes les parties intéressées DEVRAIENT s'assurer qu'il existe un cœur d'espace de nom X.500 dans le monde, et que tous les noms dans cet espace de noms peuvent être résolus. (Les espaces de noms nationaux PEUVENT se construire sur le cœur d'espace de noms).

Le reste du présent document sont la justification et les détails de ces recommandations.

Les mots "DEVRAIT", "DOIT" et "PEUT", écrits en MAJUSCULES, ont la signification définie dans la RFC2119 [17]

2. Introduction

L'Internet est utilisé pour des échanges d'informations et des communications entre ses utilisateurs. Il ne peut être utilisé efficacement pour cela que si ses utilisateurs sont capables de trouver leurs adresses réciproques. Donc, l'Internet tire parti d'un service adéquat de pages blanches, c'est à dire, d'un service de répertoire offrant les informations d'adresses (Internet) qui se rapportent aux personnes et aux organisations.

Le présent document décrit la façon dont le service de pages blanches de l'Internet (abrégé à partir de maintenant en IWPS, *Internet White Pages Service*) est mieux exploité en utilisant l'expérience , les protocoles, les produits et procédures actuels.

L'expérience [2] a montré qu'un service de pages blanches fondé sur l'enregistrement par les usagers eux-mêmes ou par des serveurs centralisés tend à collecter les données de façon hasardeuse, et de plus, qu'elle collecte des données qui sont rapidement périmées et ne sont pas tenues à jour.

Les tentatives les plus sérieuses d'établir le IWPS sont fondées sur des modèles avec des bases de données réparties (locales) dont chacune détient une partie gérable des informations du IWPS. Une telle partie consiste essentiellement en toutes les informations pertinentes de IWPS provenant du sein d'une organisation particulière ou d'un fournisseur d'accès Internet et de ses utilisateurs. Par dessus les bases de données se trouve un protocole de services de répertoire qui les connecte et fournit l'accès aux utilisateurs. Aujourd'hui, X.500 est le plus populaire des protocoles de services d'annuaire sur l'Internet, connectant les informations d'adresses d'environ 1,5 millions d'individus et 3 000 organisations. Whois++ est le second protocole en popularité. X.500 et Whois++ PEUVENT aussi être utilisés pour interconnecter d'autres informations que les seules informations de IWPS, mais nous ne discutons ici que des caractéristiques de IWPS.

Note : Il y a d'autres bases de données d'adresses, non interconnectées, sur l'Internet qui sont aussi très populaires pour mémoriser des informations d'adresses sur les gens. "Ph" est un protocole populaire à utiliser avec une base de données autonome. Il y a plus de 300 bases de données Ph enregistrées sur l'Internet. L'interconnexion de bases de données est cependant très recommandée pour un IWPS, car elle assure que les données peuvent être trouvées. Donc, Ph tel qu'il est n'est pas considéré comme un bon candidat pour un IWPS, mais de futurs développements PEUVENT changer cette situation (voir la section 12).

Actuellement, X.500 DOIT être recommandé comme protocole de services d'annuaire à utiliser pour les IWPS. Cependant, des technologies futures PEUVENT rendre possible d'utiliser aussi ou à sa place d'autres protocoles.

Comme beaucoup de gens pensent que X.500 sera remplacé sur l'Internet par d'autres protocoles dans un futur proche, il DEVRAIT être mentionné ici qu'actuellement, LDAP est vu comme le composant survivant des mises en œuvre d'aujourd'hui et le principal protocole d'accès pour les services d'annuaire de demain. Dès qu"une nouvelle technologie (utilisant probablement LDAP) sera disponible et que l'expérience aura montré qu'elle fonctionne, le présent document sera mis à jour.

Un résumé des produits X.500 se trouve dans [14] (un document mis à jour régulièrement).

Les sections 3 à 7 ci-dessous contiennent des recommandations qui se rapportent à la publication des informations dans le IWPS qui sont indépendantes d'un protocole de services d'annuaire. Les sections 8 à 11 exposent les problèmes spécifiques de X.500. Dans la section 12 sont exposés certains développements futurs tels qu'ils sont prévus au moment de la rédaction du présent document.

3. Qui DEVRAIT publier les informations de IWPS et comment ?

Les informations d'IWPS sont des informations d'adresses publiques concernant des individus et des organisations. Les informations d'IWPS qui concernent un individu DEVRAIENT être publiées et conservées par une organisation qui a un lien direct et durable avec cet individu, comme dans les cas suivants :
- l'individu est employé par l'organisation qui conserve les informations,
- l'individu est inscrit dans l'université/école qui conserve les données,
- l'individu est un abonné (personnel) du service Internet du conservateur des données.

L'organisation qui conserve les données n'a pas à mémoriser ces données dans une de ses propres bases de données locales. Bien que de faire fonctionner une base de données locale dans le service X.500 ou Whois++ ne soit pas une tâche trop difficile, il est recommandé que les fournisseurs d'accès Internet fournissent des facilités de base de données pour les organisations qui parmi leurs abonnés conservent seulement une petite partie des informations d'IWPS ou qui n'ont pas assez de ressources de gestion de systèmes. Cela va encourager de telles organisations à se joindre à l'IWPS. La collecte des informations d'IWPS et leur mise à jour DEVRAIT toujours être entre les mains de l'organisation à laquelle les informations se rapportent.

Au sein des schémas actuels (nationaux) de dénomination pour X.500, les entrées sur les individus résident sous une organisation. Dans le cas des fournisseurs d'accès Internet qui détiennent les entrées de leurs abonnés, cela voudrait dire que les individus peuvent seulement être trouvés si on connaît le nom de leur fournisseur d'accès. Le problème de cette restriction pourrait être résolu en utilisant une approche plus topographique dans le schéma de dénomination de X.500, mais il sera plus vraisemblablement résolu par un futur service d'index pour les services d'annuaires, qui permettront des recherches d'individus sans noms d'organisation (voir la section 12).

4. Quelles sortes d'informations DEVRAIENT être publiées ?

Les informations à publier sur un individu DEVRAIENT au moins inclure :
- Le nom de l'individu
- L'adresse de messagerie électronique de l'individu, dans le format de la RFC-822 ; si elle n'est pas présente, d'autres informations de contact sont à inclure
- Une indication de la relation de l'individu avec le conservateur des informations.

Lorsque X.500 est utilisé comme protocole de services de répertoire, la dernière exigence PEUT être satisfaite en utilisant l'attribut "organizationalStatus" (voir [3]) ou en ajoutant un unité organisationnelle particulière à l'espace de nom X.500 local qui reflète la relation (comme ou=étudiant ou ou=employé).

De plus, d'autres informations d'adresse publiques sur les individus PEUVENT être incluses dans l'IWPS:
- le numéro de téléphone de l'individu
- le numéro de télécopie de l'individu
- l'adresse postale de l'individu
- l'URL de la page d'accueil de l'individu sur la Toile.

Dans un futur proche, ce sera aussi une bonne idée de mémoriser des informations de clé publique.

On trouvera plus d'informations sur un schéma recommandé de pages blanches de l'Internet dans "Schéma commun pour le service des pages blanches de l'Internet" [16].

Les organisations DEVRAIENT publier les informations suivantes sur elles-mêmes dans l'IWPS :
- l'URL de la page d'accueil des organisations sur la Toile
- l'adresse postale
- les numéros de télécopie
- le domaine Internet
- divers noms et abréviations pour l'organisation qu'on s'attend à ce que les gens recherchent, comme le nom dans différentes langues, et souvent le nom de domaine d'une organisation.

Les organisations PEUVENT aussi publier des numéros de téléphone et une présentation de l'organisation.

5. Gestion des données

La gestion des données, c'est-à-dire, la collecte des informations d'IWPS et leur maintien à jour, est une tâche qui NE DOIT PAS être sous estimée pour les grandes organisations. Les recommandations suivantes peuvent être faites à cet égard :

- Une organisation DEVRAIT prendre un engagement au niveau de son comité exécutif de démarrer une base de données locale avec les informations d'IWPS. Cela rendra beaucoup plus facile d'obtenir, à l'intérieur de l'organisation, la coopération des gens qui sont impliqués dans l'établissement d'un service d'annuaire.

- Une organisation DEVRAIT décider des sortes d'informations que la base de données DEVRAIT contenir et comment elle DEVRAIT être structurée. Elle DEVRAIT suivre les recommandations de l'Internet sur la structuration des informations. Au delà des critères de la section précédente, [3] et [4] DEVRAIENT être suivis si X.500 est utilisé comme protocole des services de répertoire.

- Une organisation DEVRAIT définir des critères pour la qualité des données de l'annuaire, comme les délais, la fréquence des mises à jour, l'exactitude, etc. Ces critères DEVRAIENT être communiqués dans toute l'organisation et les entités qui y contribuent DEVRAIENT s'engager sur les niveaux de qualité définis.

- Les bases de données existantes au sein d'une organisation DEVRAIENT être utilisées pour restituer les informations de l'IWPS et les informations locales, dans la plus grande mesure possible. Une organisation DEVRAIT impliquer les personnes qui entretiennent ces bases de données et s'assurer d'obtenir un engagement formel écrit de la part de ceux qui utilisent leur source de données. L'organisation DEVRAIT s'appuyer sur ces personnes, car elles ont l'expérience de la gestion et le contrôle des données locales disponibles.

- La meilleure motivation pour qu'une organisation se joigne à l'IWPS est qu'elle aura en même temps une base de données locale pour les besoins locaux. Une base de données locale PEUT contenir plus d'informations, pas nécessairement publiques, et servir à plus d'objets qu'il n'en est demandé à l'IWPS. En se connectant à l'IWPS, une

organisation DOIT "filtrer" les informations et services locaux supplémentaires qui ne sont pas destinés à l'IWPS public en utilisant le protocole de services de répertoire.

6. Questions juridiques

La plupart des pays ont des lois qui protègent la confidentialité des informations qui concernent les personnes. Elles vont des lois laxistes des USA aux exigences britanniques sur l'exactitude des informations et à la loi norvégienne qui dit qu'on ne peut publier qu'avec la permission spécifique de l'individu concerné. Tout conservateur d'informations d'IWPS DEVRAIT publier les données conformément à la loi nationale du pays dans lequel réside la base de données locale qui détient les informations.

Certaines d'entre elles sont documentées dans [5] et [1].

Un conservateur d'informations d'IWPS DEVRAIT aussi suivre certaines règles communes, même si elles ne sont pas imposées par la loi :
- ne publier que des informations correctes,
- donner aux gens la possibilité de voir les informations mémorisées sur eux-mêmes et le droit de retirer les informations ou de les faire modifier,
- ne pas publier des informations "juste parce qu'elles sont là". Publier ce qui est nécessaire et ce qu'on pense utile, et pas plus.

Étant donné le nombre de problèmes de gestion des données et juridiques qui sont impliqués dans la publication des informations d'IWPS, de bons services d'assistance sont vitaux pour que les plus petites compagnies se joignent rapidement et efficacement à l'IWPS. Les fournisseurs d'accès Internet sont invités à fournir de tels services.

7. Ne pas taxer les recherches

On pense que du fait des contraintes technologiques actuelles, taxer les utilisateurs de l'IWPS serait dommageable à la viabilité du service. Plusieurs arguments soutiennent cette idée :

- La technologie pour les micro payements n'est pas encore disponible.

- Les services d'abonnement exigent que l'abonné souscrive à plusieurs services de recherche ou que les services soient reliés "derrière la scène" par toute une série d'accords bilatéraux; les deux structures présentant des coûts de frais généraux inacceptablement élevés et augmentent le prix d'entrée au service.

- Les protocoles actuels de services de répertoires ne prennent pas en charge l'authentification à un niveau qui semblerait approprié pour un service payant.

Il est donc fortement recommandé que toutes recherches par les usagers dans l'IWPS soient gratuites. Cela ne limite, bien sûr, en aucune façon la capacité d'utiliser le même ensemble de données d'IWPS pour prendre en charge d'autres services où la facturation PEUT être appropriée.

8. Utiliser X.500

L'IWPS fondé sur le protocole X.500 a un développement relativement large. Le service actuel contient environ 1,5 million d'entrées d'individus et 3 000 organisations. Il est coordonné par Dante, un fournisseur d'accès Internet de Grande Bretagne, connu sous le nom de "NameFLOW-Paradise".

Bien que X.500 soit parfois critiqué pour le fait que ses fonctionnalités sont restreintes par la structure hiérarchique des dénominations qu'il impose, il fournit des fonctionnalités raisonnablement bonnes comme cela a été démontré dans plusieurs articles par les organisations [5], [2], [6], [7] qui font maintenant fonctionner une production d'IWPS sur X.500. Les interfaces d'utilisateur déterminent aussi les fonctionnalités qu'offre l'IWPS X.500. Elles offrent normalement des recherches dans l'IWPS sur la base des entrées d'utilisateur suivantes :
- le nom d'une personne
- le nom d'une organisation avec laquelle cette personne peut être en relation
- le nom d'un pays

En résultat, elles fournissent les informations publiquement disponibles sur la personne en question. La plupart des interfaces d'utilisateurs offrent la possibilité de faire la liste des organisations dans un pays et des usagers dans une organisation pour aider les usagers à faire leur choix d'entrées. Il PEUT aussi y avoir la possibilité d'utiliser comme entrée une partie des noms ou des noms approximatifs.

Des interfaces d'utilisateur spécifiques peuvent fournir des recherches fondées sur d'autres entrées, comme des adresses de messagerie électronique de gens ou des adresses postales d'organisations. De telles possibilités PEUVENT cependant violer les lois sur la confidentialité. La responsabilité des fournisseurs des services de répertoires PEUT alors être engagée.

Le schéma de dénominations de X.500 impose à l'exigence d'un IWPS interconnecté que toutes les entrées qui y sont mémorisées DOIVENT avoir des noms univoques (le "schéma de dénominations"). La façon la plus aisée d'y satisfaire est l'enregistrement de toutes les entrées dans une "arborescence de dénomination" avec une racine unique ; c'est la raison pour laquelle la totalité des informations dans un IWPS X.500 est parfois désignée comme "arborescence des informations d'annuaire" (DIT, *Directory Information Tree*).

Les organisations sont vivement encouragées à utiliser le protocole X.500 pour joindre l'IWPS. Le service actuel se fonde sur la norme X.500 1988 [8] et quelques ajouts spécifiques de l'Internet au protocole qui connecte les bases de données locales [10] et au protocole d'accès [9]. Les organisations DEVRAIENT utiliser le logiciel X.500 fondé sur ces spécifications et de plus prendre en charge [11] pour le transport des protocoles OSI sur l'Internet.

Les organisations PEUVENT se connecter à l'infrastructure NameFLOW-Paradise avec des agents de système de répertoire (DSA, *Directory System Agent*) 1988 qui ne mettent pas en œuvre [10], mais il leur manquera la réplication automatique des références de connaissances. Cela sera un inconvénient, mais pas un gros problème. La norme 1993 de X.500 comporte les fonctionnalités de [10], mais utilise un protocole différent. Donc, les organisations qui se connectent à l'infrastructure avec un DSA 1993 vont aussi rencontrer cet inconvénient. La Section 12 "Développements futurs" explique pourquoi l'infrastructure n'utilise pas la norme de 1993 pour le moment.

Pour des recommandations sur les attributs à utiliser dans X.500 et comment les utiliser (pour les informations d'IWPS public ou pour les informations locales supplémentaires) le lecteur est invité à se référer à [3] et [4]. Pour des besoins locaux spécifiques non publics de nouveaux attributs (et des classes d'objets) PEUVENT aussi être définis. Il DEVRAIT être généralement recommandé d'utiliser autant que possible la capacité des attributs de X.500 à emprunter des valeurs multiples car cela améliorera considérablement la fonction de recherche du service. Par exemple, l'attribut organizationalName qui contient le nom d'une organisation ou l'attribut commonName qui contient le nom d'une personne DEVRAIT contenir tous les alias connus pour l'organisation ou la personne. En particulier, il est important d'ajouter des variantes "lisibles" de tous les attributs qu'on s'attend que les gens recherchent, si ils contiennent des caractères nationaux.

Une autre recommandation qui peut être faite est que la réplication des données [10] entre les bases de données locales soit utilisée afin d'améliorer les performances du service. Comme la duplication de toutes les entrées d'une partie de l'IWPS d'une base de données locale dans une autre PEUT violer les lois locales sur la confidentialité, il est recommandé de limiter la duplication au pays et aux entrées d'organisation et aux références de connaissances (qui disent où aller pour telle partie de l'IWPS). Bien sûr, les lois sur la confidentialité ne sont pas violées lorsque la base de données qui duplique est gérée par la même organisation que celle qui conserve les informations. Ainsi la duplication en local entre deux bases de données au sein de la même organisation est fortement recommandée.

En général, la duplication au sein du même pays posera normalement moins de problèmes juridiques qu'à travers des frontières.

On trouvera des recommandations pour le fonctionnement d'une base de données dans l'infrastructure X.500 dans [12].

L'utilisation de X.500 n'est pas recommandée pour :
- Un service de pages jaunes avec une large portée. Voir [5].
- Des recherches en dehors des cadres limités définis ici, en particulier la recherche d'une personne dont on ne sait pas à quelle organisation elle pourrait appartenir.
- Publier des informations dans d'autres jeux de caractères que l'US-ASCII, certaines des écritures européennes fondées sur le latin et le japonais (Les jeux de caractères T.61). Bien que la prise en charge de ces jeux de caractères soit disponible dans les versions révisées de X.500, les produits qui prennent en charge la révision ne sont pas encore couramment disponibles.

9. Utiliser l'espace de noms mondial

Certaines personnes ont décidé d'utiliser X.500 ou des services de style X.500, par exemple lorsque ils utilisent des serveurs Novell 4, comme un mécanisme interne de dénominations, sans coordination avec une source extérieure.

Cela pose les mêmes problèmes que l'utilisation d'adresses IP privées, avec en plus celui que les données PEUVENT devoir subir une restructuration significative lorsque on va décider de les exposer au monde extérieur.

Un service X.500 à accès mondial exige un espace de noms X.500 à connexion mondiale. Voir dans [3] et [4] les recommandations sur la façon de créer une partie locale de l'espace de noms mondial.

Bien que la norme ne soit pas très claire sur ce point et que la version la plus récente (1993) paraisse ne pas le prendre en charge, en pratique, l'espace de noms X.500 n'est gérable que si il y a un contexte de racine unique fonctionnant selon un accord de coopération. Cependant, on peut être sûr qu'il y aura des batailles acharnées pour son contrôle.

Si la décision de ce conflit ne se règle pas en faveur du service qui fonctionne actuellement, l'effet sur la qualité du service sera ruineux.

Le présent document invite toutes les parties prenantes à ne pas modifier les pratiques existantes jusqu'à ce qu'on se mette d'accord sur un meilleur système et qu'il soit prêt à entrer en fonction ; pour le moment, le contexte de racine est géré par le service NameFLOW-Paradise de Dante.

On trouvera plus d'informations sur le service NameFLOW-Paradise de Dante à l'URL
http://www.dante.net/nameflow.html

10. Utilisation de LDAP

Pour le moment, LDAP tel que documenté dans [9] est le protocole qui offre le plus de fonctionnalités de X.500 dans les endroits où il n'est pas possible de mettre en œuvre la pile OSI complète.

Il est mis en œuvre sur de nombreuses plates-formes, y compris plusieurs plates-formes de type PC, et il est populaire dans une multitude d'offres commerciales.

Un effort concerté pour rendre LDAP disponible est la méthode de publication qui donne le plus large accès aux données.

De plus, les DSA X.500 DOIVENT mettre en œuvre les liaisons nécessaires pour assurer qu'ils sont correctement intégrés dans l'arborescence de dénominations ; dans la plupart des cas, cela va signifier qu'ils DEVRAIENT mettre en œuvre au moins le protocole DSP X.500.

(La question est de savoir si une passerelle LDAP à DAP ou DAP à LDAP est pertinente dans ce contexte ; il PEUT être assez approprié de mémoriser les données sur un serveur dédié à LDAP et de le rendre disponible à l'univers DAP/DSP à travers une passerelle si les utilisateurs majeurs utilisent tous LDAP)

11. Rendre les services disponibles

L'investissement technique pour faire fonctionner un service X.500 n'est pas énorme, voir par exemple [5].

12. Développements futurs

Aujourd'hui [octobre 1996] on peut attendre plusieurs améliorations de la technologie IWPS.

La plus importante à mentionner ici est la création d'un "protocole commun d'indexation" qui DOIT permettre l'intégration de X.500, de Whois++ et des protocoles qui utilisent des bases de données autonomes. Un tel protocole ne devrait pas seulement permettre l'intégration mais devrait offrir en même temps la possibilité d'explorer les services de pages jaunes et des recherches avancées, même si elle n'utilisent que X.500.

Dans le contexte du protocole commun d'indexation, les serveurs LDAP autonomes qui sont annoncés par plusieurs

concepteurs de logiciels devraient être mentionnés. On peut accéder par LDAP à ces bases de données d'adresses autonomes. Actuellement, une version accessible librement au public est disponible sur le site de l'Université du Michigan. Est aussi annoncée une passerelle LDAP/AP qui peut intégrer un serveur LDAP autonome dans une infrastructure X.500.

D'autres améliorations comportent de définir un schéma central commun pour plusieurs services de pages blanches, conduisant à la possibilité d'accéder à des données dans plusieurs services à travers un seul protocole d'accès.

La version 1993 de la Recommandation UIT-T X.500 a déjà été mise en œuvre dans plusieurs produits. C'est une amélioration de plusieurs aspects de la norme de 1988, mais elle n'a pas encore été mise en œuvre dans l'infrastructure NameFLOW-Paradise. La principale raison en est que la norme ne reconnaît pas l'existence d'un DSA à racine unique, mais suppose que les gestionnaires des DSA de premier niveau (les DSA de pays) souscrivent des contrats bilatéraux pour les interconnexions. Dans le cas de NameFLOW-Paradise, une telle situation serait ingérable. Dans [13], une amélioration de la norme de 1993 est proposée pour rendre possible une racine unique. Aussitôt que des mises en œuvre de [13] seront disponibles, NameFLOW-Paradise expérimentera les DSA 1993. Cela est prévu en 1997.

Une fois que ces développements seront stables, ils pourront être référencés par des versions ultérieures de ce document.

13. Considérations pour la sécurité

Les implications pour la sécurité de la possession d'un répertoire sont nombreuses :
- Les gens vont avoir une façon normalisée pour accéder aux informations publiées.
- Les gens seront capables de rassembler les parties des informations dans des buts que vous n'avez pas prévu (comme de publier des annuaires, construire des moteurs de recherche, débaucher des salariés, ou faire du harcèlement téléphonique).
- Les gens vont tenter d'accéder à plus d'informations que vous n'avez l'intention d'en publier, en essayant de casser les fonctions de sécurité ou en espionnant les conversations que d'autres utilisateurs ont avec le répertoire.
- Si la modification est possible sur la Toile, les gens vont tenter de changer vos informations de façons inattendues. Les utilisateurs vont parfois aussi changer des données par erreur ; toutes les modifications indésirables ne sont pas hostiles.

La première défense pour la sécurité des répertoires est de limiter votre publication au matériel dont la disponibilité au public ne peut pas vous causer de tort, quoi qu'il arrive.

La seconde défense implique d'essayer d'imposer le contrôle d'accès. LDAP prend en charge quelques méthodes de contrôle d'accès, qui incluent l'utilisation de mots de passe en clair. Les mots de passe en clair ne sont pas un mécanisme sûr en présence d'espions ; le présent document encourage l'utilisation de mécanismes plus forts si la modification est disponible sur l'Internet public. Autrement, les droits de modification DEVRAIENT être restreints à l'intranet local.

La troisième défense implique d'essayer d'empêcher l'accès "inapproprié" au répertoire en limitant le nombre d'éléments de recherche retournés ou en refusant les opérations de liste lorsque elles ne sont pas utiles pour empêcher la "pêche au lancer". De telles défenses sont rarement complètement efficaces, parce qu'il est très difficile d'établir les limites qui différentient un utilisateur innocent qui fait des recherches inutiles et un pêcheur de données malveillant qui fait des recherches soigneusement délimitées.

Des améliorations futures PEUVENT inclure d'utiliser des sessions chiffrées, des connexions utilisant une clé publique et des demandes signées ; de tels mécanismes ne sont pas généralement disponibles aujourd'hui.

14. Remerciements

Les auteurs souhaitent remercier les personnes suivantes de leurs contributions constructives au texte du présent document :
Peter Bachman <peterb@suport.psi.com>
David Chadwick <D.W.Chadwick@iti.salford.ac.uk>
William Curtin <curtinw@ncr.disa.mil>
Patrik Faltstrom <paf@swip.net>
Rick Huber <rvh@att.com>
Thomas Lenggenhager <lenggenhager@switch.ch>
Sri Saluteri <sri@qsun.ho.att.com>
Mark Wahl <M.Wahl@critical-angle.com>

15. Glossaire

DAP *(Directory Access Protocol)* protocole d'accès à un répertoire ; utilisé entre un DUA et un DSA pour accéder aux informations d'un répertoire. Fait partie de X.500.

DSP *(Directory System Protocol)* protocole de système de répertoire : c'est le protocole utilisé entre deux DSA.

DSA *(Directory System Agent)* agent de système de répertoire – entité qui fournit aux DUA et autres DSA l'accès aux informations mémorisées dans le répertoire.

LDAP *(Lightweight Directory Access Protocol)* protocole léger d'accès à un répertoire – défini par la RFC1777.

On trouvera d'autres termes dans la RFC1983.

16. Références

[1] Jeunik, E. and E. Huizer. "Directory Services and Privacy Issues". Proceedings of Joint European Networking Conference 1993, Trondheim, http://www.surfnet.nl/surfnet/diensten/x500/privacy.html *(lien mort)*

[2] B. Jennings, "Construction d'un service d'annuaire X.500 aux USA", RFC1943**,** mai 1996. *(Information)*

[3] P. Barker, S. Kille, T. Lenggenhager, "Lignes directrices pour la dénomination et la structuration de pilotes d'annuaire X.500", RFC1617, mai 1994. *(Information)*

[4] P. Barker et S. Kille, "Schéma X.500 COSINE et Internet", RFC1274, novembre 1991. *(Remplacée par* RFC4524*)*

[5] "Introducing a Directory Service", rapport SURFnet 1995 (voir à http://info.nic.surfnet.nl/surfnet/projects/x500/introducing/ *(lien mort)*

[6] Paradise International Reports, University College London, avril 1991 - avril 1994

[7] G. Michaelson et M. Prior, "Lignes directrices pour les dénominations pour le service d'annuaire AARNet X.500", RFC1562, décembre 1993. *(Info.)*

[8] Livre bleu du CCITT, Volume VIII - Fascicule VIII. 8 novembre 1988

[9] W. Yeong, T. Howes, S. Kille, "Protocole léger d'accès de répertoire", RFC1777, mars 1995. *(Obsolète, voir* RFC3494*) (Historique)*

[10] S. Hardcastle-Kille, "Extensions de duplication et d'opérations réparties pour la fourniture d'un annuaire Internet utilisant X.500", RFC1276, novembre 1991. *(Historique)*

[11] M. Rose et D. Cass, "Services de transport ISO par dessus TCP version 3", RFC1006, STD 35, mai 1987.(*Remplace* RFC983, *MàJ par* RFC2126)

[12] R. Wright, A. Getchell, T. Howes, S. Sataluri, P. Yee, W. Yeong, "Recommandations pour un service d'annuaire X.500 de qualité", RFC1803, juin 1995. *(Information)*

[13] D. Chadwick, "Gestion du contexte de dénomination de racine X.500", RFC2120, mars 1997. *(Expérimentale)*

[14] A. Getchell, S. Sataluri, éditeurs., "Catalogue révisé des mises en œuvre X.500 disponibles", RFC1632, mai 1994. *(Information, remplacée par la RFC 2116.*

[15] The North American Directory Forum, "Schéma de dénomination pour c=US", RFC1255, septembre 1991. (*Remplace la* RFC1218, *remplacée par la* RFC1417) *(Information)*

[16] T. Genovese, B. Jennings, "Schéma commun pour le service des pages blanches de l'Internet", RFC2218, octobre 1997. *(P.S.)*

[17] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", RFC2119, BCP 14, mars 1997.

17. Adresse des auteurs

Harald Tveit Alvestrand
UNINETT
P.O.Box 6883 Elgeseter
N-7002 TRONDHEIM
NORWAY
téléphone : +47 73 59 70 94
mél : Harald.T.Alvestrand@uninett.no

Peter Jurg
SURFnet
P.O.Box 19035
NL-3501 DA UTRECHT
THE NETHERLANDS
télépho,e : +31 30 2305305
mél : Peter.Jurg@surfnet.nl