Groupe de travail Réseau
Request for Comments : 3040
Catégorie : Information
Traduction Claude Brière de L'Isle

I. Cooper, Equinix, Inc.
I. Melve, UNINETT
G. Tomlinson, CacheFlow Inc.
janvier 2001

Taxonomie de la duplication et de la mise en antémémoire sur la Toile

Statut de ce mémoire
Le présent mémoire fournit des informations pour la communauté de l'Internet. Il ne spécifie aucune norme de l'Internet. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé
Le présent mémoire spécifie la terminologie standard et la taxonomie de la duplication et de l'infrastructure de mise en antémémoire sur la Toile telles qu'elles sont utilisées aujourd'hui. Il introduit les concepts standard et les protocoles utilisés aujourd'hui au sein de ce domaine d'application. Il présente les solutions actuellement déployées qui emploient ces technologies pour établir une taxonomie standard. Les problèmes connus avec les mandataires de mise en antémémoire sont traités dans le document intitulé "Problèmes connus de mandataire/antémémoire dans HTTP" (RFC 3143), et ne sont pas abordés dans le présent document. Le présent document présente les protocoles ouverts et référence le matériel publié pour chaque protocole.

Table des Matières

1. Introduction

Depuis son introduction en 1990, la Toile mondiale *(WWW, World-Wide Web)* a évolué d'un modèle simple client-serveur en une architecture répartie complexe. Cette évolution a été largement conduite par les problèmes d'échelle associés à cette croissance exponentielle. Des paradigmes et solutions distincts ont émergé pour satisfaire des exigences spécifiques. Deux composants centraux d'infrastructure qui ont été employés pour satisfaire à cette demande de croissance sont la réplication et la mise en antémémoire. Dans de nombreux cas, il y a un besoin de services d'antémémoire sur la Toile et de réplication capables de coexister.

Le présent mémoire spécifie la terminologie standard et la taxonomie de la réplication et de l'infrastructure de mise en antémémoire déployées aujourd'hui dans l'Internet. Le principal but de ce document est d'établir une compréhension et un point de référence communs de ce domaine d'application.

Il est aussi prévu que le présent document soit utilisé à la création d'un cadre architectural standard pour un service efficace, fiable et prévisible dans une toile qui comporte à la fois des réplications et des antémémoires.

Certains des protocoles qu'examine le présent mémoire ne sont spécifiés que par des documents techniques internes de sociétés privées ou par des document en cours d'élaboration. De telles références sont incluses pour démontrer l'existence de tels protocoles, leur développement expérimental dans l'Internet d'aujourd'hui, ou pour aider le lecteur dans sa compréhension de ce domaine technologique.

De nombreux protocoles, aussi bien ouverts que propriétaires, sont employés aujourd'hui dans la réplication et la mise en antémémoire sur la Toile. La majorité des protocoles ouverts inclut le DNS [8], Cache Digests [21][10], CARP [14], HTTP [1], ICP [2], PAC [12], SOCKS [7], WPAD [13] et WCCP [18][19]. Ces protocoles, et leur utilisation au sein des environnements d'antémémoire et de réplication, sont présentés ci-dessous.

2. Terminologie

La terminologie qui suit donne les définitions des termes courants utilisés dans la communauté de la réplication et de la mise en antémémoire de la Toile. Les termes de base sont tirés, lorsque c'est possible, de la spécification HTTP/1.1 [1] et sont inclus ici pour référence. Les dérivés de premier et de second ordre sont construit à partir de ces termes de base pour aider à définir les relations qui existent dans ce domaine.

Les termes qui sont d'usage courant et sont contraires aux définitions de la RFC 2616 sont précisés.

2.1 Termes de base

La majorité de ces termes est tirée telle quelle de la RFC 2616 [1], et ils sont inclus ici pour référence.

client (tiré de [1])
Programme qui établit des connexions dans le but d'envoyer des demandes.

serveur (tiré de [1])
Programme d'application qui accepte des connexions afin de servir des demandes en renvoyant des réponses. Tout programme peut être capable de jouer à la fois les rôles de client et de serveur ; notre utilisation de ces termes se réfère seulement au rôle joué par le programme pour une connexion particulière, plutôt qu'aux capacités générales du programme. De même, tout serveur peut agir comme serveur d'origine, mandataire, passerelle, ou tunnel, changeant de comportement sur la base de la nature de chaque demande.

mandataire *(proxy)* (tiré de [1])
Programme intermédiaire qui agit à la fois comme serveur et comme client pour formuler des demandes au nom d'autres clients. Les demandes sont servies en interne ou en les repassant, avec une éventuelle traduction, aux autres serveurs. Un mandataire DOIT mettre en œuvre les exigences de la présente spécification aussi bien pour le client que pour le serveur. Un "mandataire transparent" est un mandataire qui ne modifie pas la demande ou réponse au delà de ce qui est exigé pour l'authentification et l'identification du mandataire. Un "mandataire non transparent" est un mandataire qui modifie la demande ou réponse afin de fournir un complément de service à l'agent d'utilisateur, comme des service d'annotation de groupe, une transformation du type de support, une réduction de protocole, ou un filtrage d'anonymat. Sauf lorsque qu'un

comportement transparent ou non transparent est explicitement déclaré, les exigences du mandataire HTTP s'appliquent aux deux types de mandataires.

Note : le terme de "mandataire transparent" se réfère à un mandataire sémantiquement transparent tel que décrit dans [1], et non à ce qui est habituellement compris dans la communauté de la mise en antémémoire. Nous recommandons que le terme "mandataire transparent" soit toujours muni d'un qualificatif pour éviter la confusion (par exemple, "mandataire transparent du réseau"). Voir cependant la définition de "mandataire d'interception" ci-dessous.

La condition ci-dessus qui requiert la mise en œuvre à la fois des exigences de serveur et de client de HTTP/1.1 n'est appropriée que pour un mandataire transparent hors réseau.

antémémoire (tiré de [1])
Mémorisation locale d'un programme pour les messages de réponse et le sous-système qui contrôle sa mémorisation de messages, leur restitution, et leur suppression. Une antémémoire mémorise les réponses qui peuvent être mises en antémémoire afin de réduire le temps de réponse et la consommation de bande passante du réseau sur les demandes futures, équivalentes. Tout client ou serveur peut inclure une antémémoire, bien qu'une antémémoire ne puisse être utilisée par un serveur agissant comme tunnel.

Note : Le terme "antémémoire" utilisé seul signifie souvent une "antémémoire mandataire".

Note : Il y a des motifs supplémentaires à la mise en antémémoire, par exemple de réduire la charge du serveur (comme un moyen supplémentaire de réduction du temps de réponse).

mettable en antémémoire (tiré de [1])
Une réponse est mettable en antémémoire si une antémémoire est autorisée à mémoriser une copie du message de réponse pour l'utiliser à répondre à des demandes ultérieures. Les règles de détermination de la mise en antémémoire des réponses HTTP sont définies à la Section 13. Même si une ressource est mettable en antémémoire, il peut y avoir des contraintes supplémentaires concernant l'utilisation par une antémémoire de la copie qu'elle détient pour une demande particulière.

routeur (tiré de [1])
Un serveur qui agit comme un intermédiaire pour un autre serveur. À la différence d'un mandataire, un routeur reçoit des demandes comme si il était le serveur d'origine pour la ressource demandée ; le client demandeur peut ne pas savoir qu'il communique avec un routeur.

tunnel (tiré de [1])
Un programme intermédiaire qui agit comme un relais aveugle entre deux connexions. Une fois actif, un tunnel n'est pas considéré comme partie de la communication HTTP, bien que le tunnel puisse avoir été initié par une demande HTTP. Le tunnel cesse d'exister lorsque les deux extrémités des connexions relayées sont closes.

réplication
"Création et maintien d'une copie dupliquée d'une base de données ou système de fichiers sur un ordinateur différent, normalement un serveur." – Dictionnaire libre en ligne de l'informatique (FOLDOC, *Free Online Dictionary of Computing*)

entrant/sortant (tiré de [1])
Entrant et sortant se réfère aux chemins de demande et de réponse des messages : "entrant" signifie "qui voyage vers le serveur d'origine", et "sortant" signifie "qui voyage vers l'agent d'utilisateur".

élément de réseau
Un appareil du réseau qui introduit plusieurs chemins entre source et destination, transparent à HTTP.

2.2 Termes dérivés de premier ordre

Les termes suivants sont construits en se fondant sur les termes de base ci-dessus.

serveur d'origine (tiré de [1])
C'est le serveur sur lequel réside ou va être créée une ressource donnée.

agent d'utilisateur (tiré de [1])
C'est le client qui initie une demande. Ce sont souvent des navigateurs, des éditeurs, des robots araignées (robots de traversé de la toile), ou autres outils d'utilisateur final.

mandataire de mise en antémémoire
Un mandataire avec une antémémoire, agissant comme un serveur pour les clients, et comme client pour les serveurs. Les mandataires d'antémémoire sont souvent appelés "antémémoires mandataires" ou simplement "antémémoires". Le terme "mandataire" est aussi fréquemment utilisé à tort pour parler de mandataires de mise en antémémoire.

substitut *(surrogate)*
Routeur co-localisé avec un serveur d'origine, ou situé à un point différent dans le réseau, qui a reçu délégation d'autorité pour agir au nom d'un ou plusieurs serveurs d'origine et fonctionne normalement en étroite coopération avec eux. Les réponses sont normalement délivrées à partir d'une antémémoire interne. Les substituts peuvent déduire les entrées d'antémémoire du serveur d'origine ou d'un autre des délégués du serveur d'origine. Dans certains cas un substitut peut tunneler de telles demandes. Lorsque il existe une étroite coopération entre les serveurs d'origine et les substituts, cela permet des modifications de certaines exigences de protocole, y compris les directives Cache-Control *(contrôle d'antémémoire)* de [1]. De telles modifications ont déjà été entièrement spécifiées. Les appareils communément appelés "mandataires inverses" et "accélérateurs de serveur (d'origine)" sont tous deux plus correctement définis comme substituts.

mandataire inverse *(reverse proxy)*
Voir à "substitut".

accélérateur de serveur *(server accelerator)*
Voir à "substitut".

2.3 Dérivés de second ordre

Les termes suivants s'appuient sur les dérivés du premier ordre :

serveur maître d'origine
Un serveur d'origine sur lequel réside la version définitive d'une ressource.

serveur réplique d'origine
Un serveur d'origine qui détient une réplique d'une ressource, mais qui peut agir comme référence d'autorité pour les demandes de client.

consommateur de contenu
L'utilisateur ou le système qui initie des demandes entrantes, par l'utilisation d'un agent d'utilisateur.

navigateur *(browser)*
Une instance spéciale d'agent d'utilisateur qui agit comme un appareil de présentation de contenu pour le consommateur de contenu.

2.4 Termes topologiques

Les définitions suivantes sont ajoutées pour décrire la topologie d'appareil de mise en antémémoire :

antémémoire d'agent d'utilisateur
L'antémémoire au sein du programme d'agent d'utilisateur.

mandataire de mise en antémémoire local
Le mandataire de mise en antémémoire auquel un agent d'utilisateur se connecte.

mandataire de mise en antémémoire intermédiaire
Du point de vue du consommateur de contenu, toutes les antémémoires qui participent au maillage d'antémémoire qui ne sont pas le mandataire de mise en antémémoire local de l'agent d'utilisateur.

serveur d'antémémoire
Un serveur pour les demandes faites par les mandataire de mise en antémémoire locaux et intermédiaires, mais qui n'agit pas comme un mandataire.

dispositif d'antémémoire *(cache array)*
Une grappe de mandataires de mise en antémémoire qui agissent logiquement comme un service et partagent l'espace de nom de ressource à travers le dispositif. Aussi appelé "dispositif diffusé" ou "grappe d'antémémoire".

maillage d'antémémoire *(caching mesh)*
Ensemble à couplage lâche de mandataires coopérants et (facultativement) de serveurs de mise en antémémoire, ou de grappes, agissant indépendamment mais partageant du contenu mettable en antémémoire entre eux en utilisant des protocoles de communication inter antémémoires.

2.5 Utilisation automatique de mandataires

Les administrateurs de réseau peuvent souhaiter forcer ou faciliter l'utilisation de mandataires par les clients, en activant une telle configuration au sein du réseau lui-même ou au sein de systèmes automatiques dans les agents d'utilisateur, de telle sorte que le consommateur de contenu n'ait pas besoins de connaître de tels problèmes de configuration.

Les termes qui décrivent de telles configurations sont donnés ci-dessous.

configuration automatique de mandataire d'agent d'utilisateur
C'est la technique de découverte de la disponibilité d'un ou plusieurs mandataires et la configuration automatisée de l'agent d'utilisateur pour s'en servir. L'utilisation d'un mandataire est transparent pour le consommateur de contenu mais pas pour l'agent d'utilisateur. Le terme de "configuration automatique de mandataire" est aussi utilisé dans ce sens.

interception de trafic
C'est le processus d'utilisation d'un élément de réseau pour examiner le trafic réseau afin de déterminer si il devrait être redirigé.

redirection de trafic
C'est la redirection des demandes du client à partir d'un élément de réseau qui effectue l'interception de trafic vers un mandataire. Utilisé pour déployer des mandataires (mettre en antémémoire) sans qu'il soit besoin de reconfigurer manuellement les agents d'utilisateur individuels, ou de forcer l'utilisation d'un mandataire lorsque une telle utilisation ne surviendrait pas sans cela.

mandataire d'interception (aussi dit "mandataire transparent", "antémémoire transparente")
Le terme de "mandataire transparent" a été utilisé au sein de la communauté des antémémoires pour décrire les mandataires utilisés avec zéro configuration au sein de l'agent d'utilisateur. Une telle utilisation est assez transparente pour les agents d'utilisateur. Du fait de discordances avec [1] (voir la définition de "mandataire" ci-dessus), et d'objections à l'utilisation du mot "transparent", nous introduisons le terme de "mandataire d'interception" pour décrire les mandataires qui reçoivent les flux de trafic redirigé depuis les éléments de réseau qui effectuent l'interception de trafic. Les mandataires d'interception reçoivent les flux de trafic entrants à travers le processus de redirection de trafic. (De tels mandataires sont déployés par les administrateurs de réseau pour faciliter ou exiger l'utilisation des services appropriés offerts par le mandataire). Les problèmes associés au déploiement des mandataires d'interception sont décrits dans le document "Problèmes connus de mandataire/antémémoire dans HTTP" [23]. L'utilisation des mandataires d'interception n'exige aucune configuration de la part de l'agent d'utilisateur qui agit comme si il communiquait directement avec un serveur d'origine.

3. Relations de système réparti

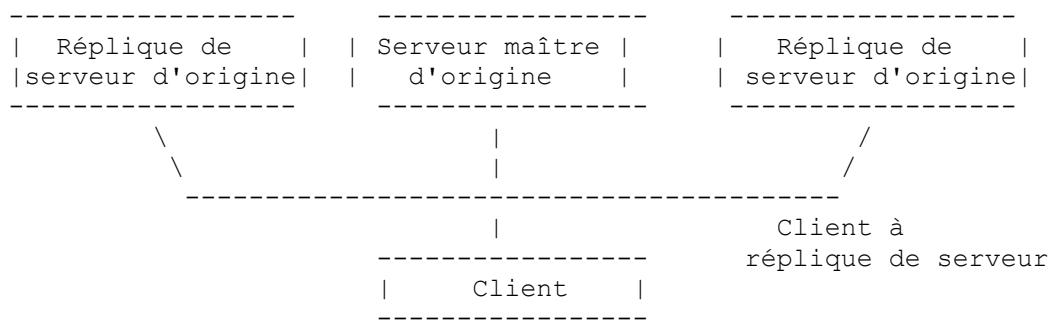
La présente section identifie les relations qui existent dans un environnement réparti de réplication et de mise en antémémoire. Après avoir défini ces relations, les sections suivantes décrivent les protocoles de communication utilisés dans chaque relation.

3.1 Relations de réplication

Les paragraphes suivants décrivent les relations entre les clients et les répliques et entre les répliques elles-mêmes.

3.1.1 De client à réplique

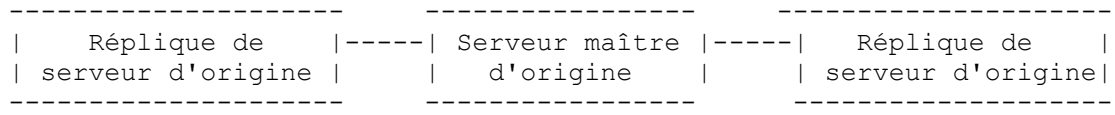
Un client peut communiquer avec une ou plusieurs répliques de serveur d'origine, aussi bien qu'avec des serveurs maîtres d'origine. (En l'absence de répliques de serveurs le client interagit directement avec le serveur d'origine comme dans le cas normal.)



Les protocoles utilisés pour permettre au client d'utiliser une des répliques se trouvent à la Section 4.

3.1.2 Inter-réplique

C'est la relation entre le ou les serveurs d'origine et les répliques de serveur d'origine, pour dupliquer les ensembles de données auxquels accèdent les clients dans la relations indiquée au paragraphe 3.1.1.



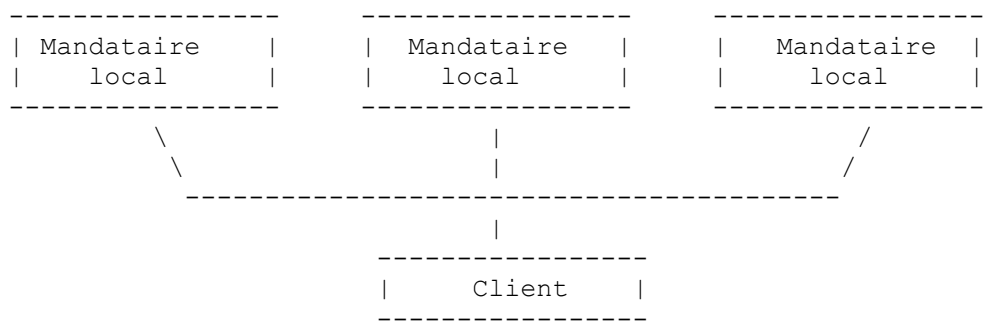
Les protocoles utilisés dans cette relation se trouvent à la Section 5.

3.2 Relations de mandataire

Les mandataires (de mise en antémémoire et les serveurs d'antémémoire communiquent de diverses façons les uns avec les autres, et avec les agents d'utilisateur.

3.2.1 De client à mandataire de non interception

Un client peut communiquer avec zéro, un ou plusieurs mandataires pour certaines demandes ou toutes. Lorsque le résultat de la communication n'utilise aucun mandataire, la relation est entre le client et le serveur (réplique) d'origine (voir au paragraphe 3.1.1).

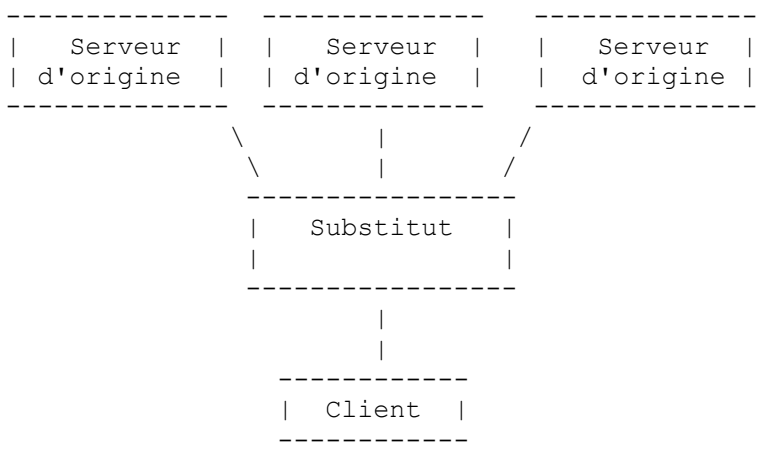


De plus, un agent d'utilisateur peut interagir avec un serveur supplémentaire – qui fonctionne au nom d'un mandataire pour les besoins de la configuration automatique de mandataire d'agent d'utilisateur.

Les schémas et protocoles utilisés dans ces relations se trouvent à la Section 6.

3.2.2 Client à substitut de serveur d'origine

Un client peut communiquer avec zéro, un ou plusieurs substituts pour des demandes destinées à un ou plusieurs serveurs d'origine. Lorsque on n'utilise pas de substitut, le client communique directement avec un serveur d'origine. Lorsque un substitut est utilisé, le client communique comme si c'était avec un serveur d'origine. Le substitut satisfait la demande à partir de son antémémoire interne, ou agit comme un routeur ou un tunnel vis à vis du serveur d'origine.

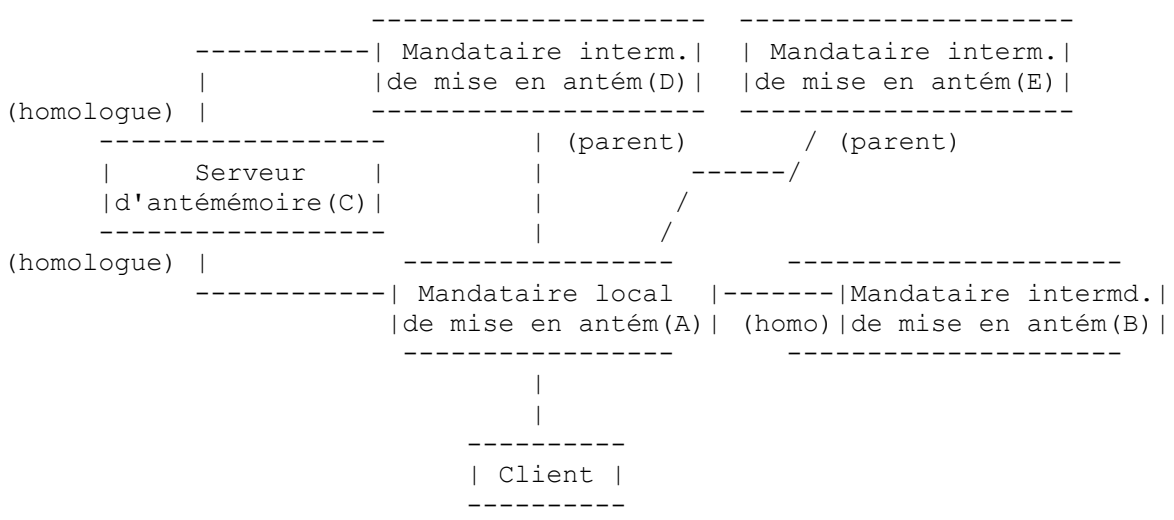


3.2.3 Inter mandataires

Les relations inter mandataires existent comme maillages (couplage lâche) et comme grappes (couplage serré).

3.2.3.1 Maillage de mandataire (de mise en antémémoire)

Au sein d'un maillage à couplage lâche de mandataires (de mise en antémémoire) la communication peut se faire au même niveau entre homologues, et avec un ou plusieurs parents.



Le client n'est inclus que pour les besoins de l'illustration

Une demande entrante peut être acheminée à un des nombreux mandataires intermédiaires (de mise en antémémoire) sur la base de la détermination que ce parent est mieux placé pour résoudre la demande.

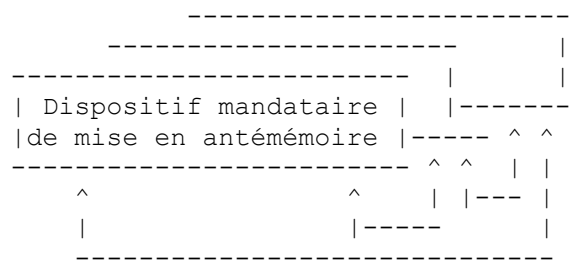
Par exemple, dans la figure ci-dessus, le serveur d'antémémoire C et le mandataire intermédiaire de mise en antémémoire B sont les homologues du mandataire local de mise en antémémoire A, et ne peuvent être utilisés que lorsque la ressource demandée par A existe déjà sur B ou C. Les mandataires intermédiaires de mise en antémémoire D et E sont parents de A, et c'est le choix de A d'utiliser l'un d'eux pour résoudre une demande particulière.

La relation entre A et B n'a de sens que dans un environnement de mise en antémémoire, alors que les relations entre A et D et entre A et E sont aussi appropriées lorsque D ou E sont des mandataires qui ne font pas de mise en antémémoire.

Les protocoles utilisés dans ces relations se trouvent au paragraphe 7.1.

3.2.3.2 Dispositifs mandataires (de mise en antémémoire)

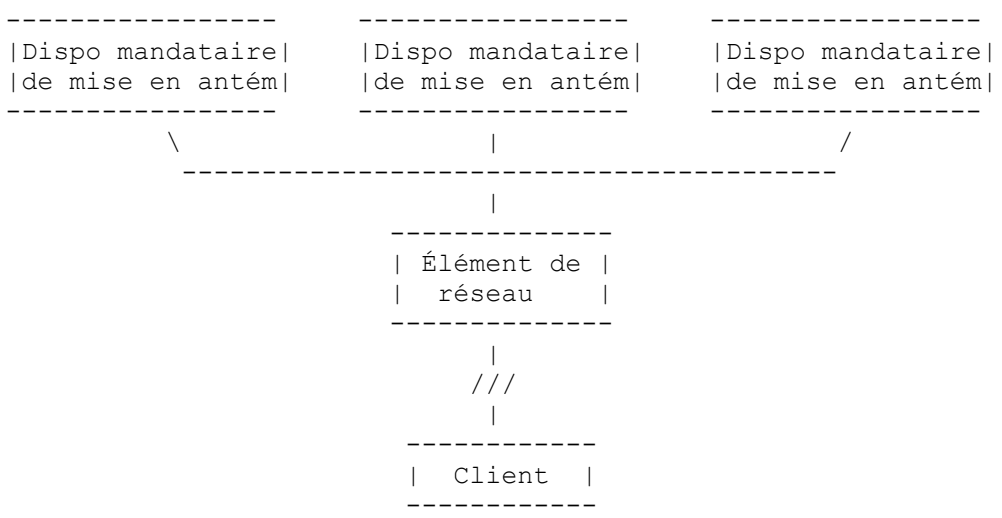
Lorsque un agent d'utilisateur peut avoir une relation avec un mandataire, il est possible qu'il ait à la place une relation avec un dispositif de mandataires arrangés en un maillage étroitement couplé.



Les protocoles utilisés dans cette relation se trouvent au paragraphe 7.2.

3.2.4 D'élément de réseau à mandataire de mise en antémémoire

Un élément de réseau qui effectue de l'interception de trafic peut choisir de rediriger les demandes d'un client à un mandataire spécifique au sein d'un dispositif. (Il peut aussi choisir de ne pas rediriger le trafic, auquel cas la relation est entre le client et le serveur d'origine (ou ses répliques), voir le paragraphe 3.1.1.)



Le mandataire d'interception peut être directement en ligne avec le flux de trafic - auquel cas l'élément de réseau intercepteur et le mandataire d'interception font partie du même système matériel – ou peut être hors du chemin, ce qui exige que l'élément de réseau intercepteur redirige le trafic sur un autre segment de réseau. Dans ce dernier cas, les protocoles de communication rendent l'élément de réseau intercepteur capable d'arrêter et démarrer la redirection du trafic lorsque le mandataire d'interception de vient (in)disponible. Les détails de ces protocoles se trouvent à la Section 8.

4. Sélection de réplique

La présente section décrit les schémas et protocoles utilisés dans la coopération et la communication entre client et répliques de serveur d'origine de la Toile. La situation idéale est de découvrir une réplique optimale de serveur d'origine pour communiquer avec les clients. L'optimum est une décision fondée sur une politique, souvent appuyée sur la proximité, mais qui peut se fonder sur d'autres critères tels que la charge.

4.1 Hyperliens de navigation

Meilleure référence connue : Le présent mémoire.

Description :
C'est le plus simple des mécanismes de communication du client aux répliques. Il utilise les URI d'hyperliens incorporés dans les pages de la toile qui pointent sur les répliques individuelles de serveur d'origine. Le consommateur de contenu choisit manuellement le lien qu'il souhaite utiliser avec la réplique de serveur d'origine.

Sécurité : Elle repose sur la sécurité du protocole associée au schéma d'URI approprié.

Utilisation : Probablement le mécanisme de communication le plus couramment développé avec les répliques. L'interopérabilité avec les personnes est universelle.

Auteur de la proposition : Les éditeurs du présent document.

4.2 Redirection HTTP par les répliques

Meilleure référence connue : Le présent mémoire

Description :
Mécanisme simple et d'utilisation courante pour connecter les clients aux répliques de serveur d'origine. Les clients sont redirigés sur une réplique optimale de serveur d'origine via les codes de réponse du protocole HTTP [1], par exemple, 302 "Trouvé", ou 307 "Redirection temporaire". Un client établit la communication HTTP avec une des répliques de serveur d'origine. La réplique de serveur d'origine contactée initialement peut alors choisir d'accepter le service ou de rediriger à nouveau le client. Se reporter au paragraphe 10.3 de HTTP/1.1 [1] pour des informations sur les codes de réponse HTTP.

Sécurité : Repose entièrement sur la sécurité HTTP.

Utilisation :
Observée dans un certain nombre de grands sites de la Toile. L'extension de son usage dans l'Internet est inconnue.

Auteur de la proposition : Les éditeurs du présent document.

4.3 Redirection par le DNS

Meilleures références connues :
* RFC 1794 Prise en charge de l'équilibrage de charge par le DNS [8]
* Le présent mémoire.

Description :
Le service des noms de domaines (DNS, *Domain Name Service*) fournit un mécanisme plus sophistiqué de communication de client à réplique. Cela est réalisé par les serveurs du DNS qui trient les adresses IP résolues sur la base des politiques de qualité de service. Lorsque un client résout le nom d'un serveur d'origine, le serveur DNS amélioré trie les adresses IP disponibles des répliques de serveur d'origine en commençant par la réplique optimale et en terminant par la réplique qui l'est le moins.

Sécurité : Repose entièrement sur la sécurité du DNS et des autres protocoles qui peuvent être utilisés dans la détermination de l'ordre de tri.

Utilisation :
Observée sur un certain nombre de grands sites de la Toile et de services de grands FAI hébergés sur la Toile. L'extension de son usage sur l'Internet est inconnue, mais on pense qu'elle est croissante.

Auteur de la proposition : Les éditeurs du présent document.

5. Communication inter répliques

La présente section décrit la coopération et la communication entre serveurs d'origine maître et répliques. Elle est utilisée pour dupliquer les ensembles de données entre les serveurs d'origine.

5.1 Duplication conduite par lots

Meilleure référence connue : Le présent mémoire

Description :
La réplique de serveur d'origine à mettre à jour initie la communication avec un serveur maître d'origine. La

communication est établie à des intervalles fondés sur des transactions mises en file d'attente qui sont programmées pour un traitement différé. Les politiques de mécanisme de programmation varient, mais sont généralement répétées à un moment spécifié. Une fois qu'une communication est établie, les ensembles de données sont copiés sur la réplique de serveur d'origine qui a pris l'initiative.

Sécurité :
S'appuis sur le protocole utilisé pour transférer l'ensemble de données. FTP [4] et RDIST sont les protocoles les plus couramment observés.

Utilisation : Très commune pour la synchronisation de sites miroirs sur l'Internet.

Auteur de la proposition : Les éditeurs du présent document.

5.2 Duplication conduite par la demande

Meilleure référence connue : Le présent mémoire

Description :
La réplique de serveur d'origine acquiert le contenu en fonction de la demande du client. Lorsque un client demande une ressource qui n'est pas dans l'ensemble de données de la réplique/substitut de serveur d'origine, elle fait une tentative pour résoudre la demande en acquérant la ressource auprès du serveur maître d'origine, et la retourne au client demandeur.

Sécurité :
S'appuis sur le protocole utilisé pour transférer les ressources. FTP [4], Gopher [5], HTTP [1] et ICP [2] sont les protocoles le plus couramment observés.

Utilisation : Observée sur plusieurs grands sites de la Toile. L'extension de son usage sur l'Internet est inconnue.

Auteur de la proposition : Les éditeurs du présent document.

5.3 Duplication synchronisée

Meilleure référence connue : Le présent mémoire

Description :
Les répliques de serveurs d'origine coopèrent en utilisant des stratégies synchronisées et des protocoles de réplique spécialisés pour garder la cohérence des ensembles de données répliquées. Les stratégies de synchronisation vont d'une cohérence étroite (de quelques minutes) à une cohérence lâche (quelques heures ou plus). Les mises à jour surviennent entre les répliques sur la base des contraintes de temps de synchronisation du modèle de cohérence employé et sont généralement seulement sous la forme de deltas.

Sécurité :
Tous les protocoles connus utilisent des méthodes d'échange de clés cryptographiques fortes, qui sont fondées sur le modèle Kerberos de secret partagé ou sur le modèle RSA de clés publique/privée.

Utilisation : Observé sur quelques sites, principalement des campus universitaires.

Auteur de la proposition : Les éditeurs du présent document.

Note : Les éditeurs connaissent au moins deux protocoles ouverts au public - AFS et CODA – ainsi que le protocole breveté NRS de Novell.

6. Configuration d'agent d'utilisateur à mandataire

La présente section décrit la configuration, coopération et communication entre agents d'utilisateurs et mandataires.

6.1 Configuration manuelle de mandataire

Meilleure référence connue : Le présent mémoire

Description :
Chaque utilisateur doit configurer son agent d'utilisateur en fournissant les informations relatives aux protocoles de mandataires et les politiques locales.

Sécurité : Le potentiel d'erreur est élevé ; chaque utilisateur règle individuellement ses préférences.

Utilisation :
Largement déployé, utilisé dans tous les navigateurs courants. La plupart des navigateurs prennent aussi en charge des options supplémentaires.

Auteur de la proposition : Les éditeurs du présent document.

6.2 **Auto configuration de mandataire** (PAC, proxy auto configuration)

Meilleure référence connue : "Navigator Proxy Auto-Config File Format" [12]

Description :
Un programme JavaScript récupéré sur un serveur de la Toile est exécuté pour chaque URL accédé pour déterminer le mandataire approprié (si il en est) à utiliser pour accéder à la ressource. Les agents d'utilisateur doivent être configurés à demander ce programme au démarrage. Il n'y a pas de mécanisme bootstrap, la configuration manuelle est nécessaire.

En dépit de la configuration manuelle, le processus de configuration du mandataire est simplifié par sa centralisation au sein d'un programme en une localisation unique.

Sécurité :
Une politique commune d'entreprise est possible mais exige quand même une configuration initiale manuelle. La PAC est mieux que la "configuration manuelle de mandataire" car les administrateurs de PAC peuvent mettre à jour la configuration du mandataire sans autre intervention de l'utilisateur.

L'interopérabilité des fichiers de PAC n'est pas très élevée, car les différents navigateurs ont des interprétations légèrement différentes du même programme, ce qui conduit éventuellement à des effets indésirables.

Utilisation : Mis en œuvre dans le navigateur Netscape et dans Internet Explorer de Microsoft.

Auteur de la proposition : Les éditeurs du présent document.

6.3 **Protocole d'acheminement à dispositif d'antémémoire** (CARP, Cache Array Routing Protocol) **v1.0**

Meilleure référence connues :
* "Protocole d'acheminement à dispositif d'antémémoire" [14] (travail en cours)
* "Spécifications du protocole d'acheminement à dispositif d'antémémoire (CARP) v1.0" [15]
* "Cache Array Routing Protocol and Microsoft Proxy Server 2.0" [16]

Description :
Les agents d'utilisateur peuvent utiliser CARP directement comme fonction de hachage sur la base d'un mécanisme de sélection de mandataire. Ils doivent être configurés avec la localisation des informations de grappe.

Sécurité : Les considérations pour la sécurité ne sont pas traitées dans la spécification en cours.

Utilisation :
Mis en œuvre dans le serveur mandataire de Microsoft, Squid. Mis en œuvre dans les agents d'utilisateur via des programmes de PAC.

Auteur de la proposition : Les éditeurs du présent document.

6.4 Protocole d'auto découverte de mandataire de la Toile (WPAD)

Meilleure référence connue :
"Protocole d'auto découverte de mandataire de la Toile (WPAD, *Web Proxy Auto-Discovery Protocol*)" [13] (travail en cours)

Description :
WPAD utilise une collection de mécanismes préexistants de découverte de ressources Internet pour effectuer l'auto découverte des mandataires de la Toile.

Le seul objectif de WPAD est de localiser l'URL du PAC [12]. WPAD ne spécifie pas quels mandataires seront utilisés. WPAD fournit l'URL de PAC, et le programme de PAC fonctionne alors comme défini ci-dessus pour choisir les mandataires sur la base de la demande de ressource.

Le protocole WPAD spécifie ce qui suit :
* comment utiliser chaque mécanisme dans le but spécifique de l'auto découverte de mandataire de la Toile
* l'ordre dans lequel les mécanismes devraient être effectués
* l'ensemble minimal de mécanisme qui doivent être tentés par un agent d'utilisateur conforme à WPAD.

Les mécanismes de découverte de ressource utilisés par WPAD sont les suivants :
* Protocole dynamique de configuration d'hôte (DHCP)
* Protocole de localisation de service (SLP)
* "Pseudonymes bien, connus" en utilisant les enregistrements A du DNS
* Enregistrements SRV du DNS
* "service : URL" dans les enregistrements TXT du DNS.

Sécurité : Repose sur la sécurité du DNS et de HTTP.

Utilisation :
Mis en œuvre dans certains agents d'utilisateurs et serveurs mandataires de mise en antémémoire. Plus de deux mises en œuvre indépendantes.

Auteur de la proposition : Josh Cohen

7. Communication inter mandataires

7.1 Communication inter mandataires à couplage lâche

La présente section décrit la coopération et la communication entre des mandataires d'antémémoire.

7.1.1 Protocole des antémémoires Internet (ICP)

Meilleure référence connue :
RFC 2186 "Protocole des antémémoires Internet (ICP), version 2" [2]

Description :
ICP est utilisé par les mandataires pour interroger d'autres mandataires (de mise en antémémoire) sur les ressources de la Toile, pour voir si la ressource demandée est présente sur l'autre système

ICP utilise UDP. Comme UDP est un protocole de transport réseau incorrect, une estimation de l'encombrement du réseau et de la disponibilité peut être calculée par les pertes de ICP. Cette mesure rudimentaire des pertes donne, avec le délai d'aller retour, une méthode d'équilibrage de charge pour les antémémoires.

Sécurité : Voir la RFC 2187 [3]

ICP ne transporte pas d'informations sur les en-têtes HTTP associés aux ressources. Les en-têtes HTTP peuvent comporter des directives de contrôle d'accès et d'antémémoire. Comme les mandataires demandent la disponibilité des ressources, et les restituent ensuite en utilisant HTTP, il peut survenir de fausses touches d'antémémoire (par exemple, l'objet est présent

dans l'antémémoire mais n'est pas accessible à un clone).

ICP souffre de tous les problèmes de sécurité de UDP.

Utilisation :
Largement déployé. La plupart des mises en œuvre courantes de mandataires d'antémémoire prennent en charge ICP d'une certaine façon.

Auteur de la proposition : Les éditeurs du présent document.

Voir aussi à : "Extension du protocole d'antémémoire de l'Internet" [17] (Travail en cours)

7.1.2 Protocole de mise en antémémoire hypertexte

Meilleure référence connue :
RFC 2756 "Protocole de mise en antémémoire hypertexte (HTCP/0.0) [9]

Description :
HTCP est un protocole de découverte des mandataires de mise en antémémoire HTTP et des données en antémémoire, de gestion d'ensembles de mandataires d'antémémoire HTTP, et de surveillance des activités d'antémémoire.

Les demandes HTCP comporte du matériel d'en-tête HTTP, alors que ICPv2 ne le fait pas, ce qui permet aux réponses HTCP de décrire plus précisément le comportement qui va résulter d'une demande HTTP ultérieure pour la même ressource.

Sécurité :
Utilise facultativement l'authentification HMAC-MD5 [11] de secret partagé. Les protocole est vulnérables aux attaques si l'authentification n'est pas utilisée.

Utilisation :
HTCP est mis en œuvre dans Squid et dans le "Web Gateway Interceptor" *(intercepteur de routeur de la Toile)*.

Auteur de la proposition : Les éditeurs du présent document.

7.1.3 Résumé d'antémémoire

Meilleures références connues :
* "Cache Digest Specification - version 5" [21] *(spécification du résumé d'antémémoire)*
* "Summary Cache: A Scalable Wide-Area Web Cache Sharing Protocol" *(Résumé d'antémémoire : un protocole échelonnable de partage d'antémémoire de large zone pour la Toile)* [10] (voir la note)

Description :
Les résumés d'antémémoire sont une réponse aux problèmes de latence et d'encombrement associés aux mécanismes de communication inter antémémoires précédents tels que le protocole d'antémémoire de l'Internet (ICP) [2] et le protocole d'antémémoire hypertexte [9]. À la différence de ces protocoles, Le résumé d'antémémoire prend en charge l'échange de flux homologues entre mandataires et serveurs d'antémémoires sans qu'un échange de demande réponse soit nécessaire pour chaque demande entrante. À la place, les autres systèmes homologues vont chercher un résumé du contenu de l'antémémoire (le Résumé). L'utilisation des résumés d'antémémoires rend possible la détermination avec un degré de précision relativement élevé de si une ressource données est en antémémoire dans un système particulier.

Résumés d'antémémoire est à la fois un protocole d'échange et un format de données.

Sécurité :
Si le contenu d'un résumé est sensible, il devrait être protégé. Toutes les méthodes qui seraient normalement appliquées pour sécuriser une connexion HTTP peuvent être appliquées aux résumés d'antémémoire.

Une attaque de "cheval de Troie" est actuellement possible dans un maillage : un système A peut construire un faux résumé d'homologue pour le système B et le servir aux homologues de B si ils le demandent. De cette façon, A peut diriger du trafic de/vers B. L'impact de ce problème est minimisé par le modèle "tiré" de transfert des résumés d'antémémoire d'un système à un autre.

Les résumés d'antémémoire permettent de connaître le contenu des antémémoires d'homologues au niveau d'une URL. Et

donc, ils n'imposent pas un niveau particulier de gestion de politique et peuvent être utilisés pour mettre en œuvre diverses politiques à tout niveau (utilisateur, entreprise, etc.).

Utilisation : Les résumés d'antémémoire sont pris en charge dans Squid.
Maillages d'antémémoire : NLANR Mesh; TF-CACHE Mesh (Réseaux universitaires européens)

Auteur de la proposition : Alex Rousskov pour [21], Pei Cao pour [10].

Note : La technologie des résumés d'antémémoire [10] est soumise à un brevet de l'Université du Wisconsin-Madison.

7.1.4 Pré remplissage d'antémémoire

Meilleure référence connue : "Pre-filling a cache - A satellite overview" [20] (Travail en cours)

Description :
Le pré remplissage d'antémémoire est une mise en œuvre de mise en antémémoire "poussée. Il est particulièrement bine adapté aux réseaux IP en diffusion groupée parce qu'il permet que des ressources présélectionnées soient simultanément insérées dans des antémémoires au sein d'un groupe de diffusion groupée ciblé. Différentes mises en œuvre de pré remplissage d'antémémoire existent déjà, en particulier dans le contexte des satellites. Cependant, il n'y a toujours pas de norme pour ce type d'antémémoire "poussée" et les fabricants proposent des solutions fondées soit sur des équipements dédiés soit sur des antémémoires du domaine public étendues par un module de pré remplissage.

Sécurité : Repose sur les protocoles inter-antémémoires utilisés.

Utilisation : Observée chez deux fournisseurs de service de distribution de contenus commerciaux.

Auteur de la proposition : Ivan Lovric

7.2 Communication inter antémémoire à couplage étroit

7.2.1 Protocole d'acheminement de dispositif d'antémémoire (CARP) v1.0

Voir aussi au paragraphe 6.3

Meilleure référence connues :
* "Cache Array Routing Protocol" [14] (travail en cours)
* "Cache Array Routing Protocol (CARP) v1.0 Specifications" [15]
* "Cache Array Routing Protocol and Microsoft Proxy Server 2.0" [16]

Description :
CARP est une fonction de hachage qui divise l'espace d'URL entre une grappe de mandataires. CARP inclut la définition d'un tableau des membres d'un dispositif de mandataires, et les moyens de télécharger ces informations.

Un agent d'utilisateur qui met en œuvre CARP v1.0 peut allouer et acheminer intelligemment les demandes pour les URL à tout membre du dispositif de mandataires. Du fait du tri résultant des demandes à travers ces mandataires, la duplication du contenu d'antémémoire est éliminé et le taux global de touche des antémémoires peut être amélioré.

Sécurité : Les considérations de sécurité ne sont pas couvertes par la spécification en cours.

Utilisation :
Mis en œuvre dans les serveurs de mandataires de mise en antémémoire. Il y a plus de deux mises en œuvre indépendantes.

Auteur de la proposition : Les éditeurs du présent document.

8. Communication d'élément de réseau

La présente section décrit la coopération et la communication entre des mandataires et des éléments de réseau. Les routeurs et les commutateurs sont des exemples de tels éléments de réseau. Ils sont généralement utilisés pour déployer des mandataires d'interception et/ou des dispositifs diffusés.

8.1 Protocole de commande d'antémémoires de la Toile (WCCP)

Meilleure référence connues :
"Web Cache Control Protocol" (WCCP, *Protocole de commande d'antémémoires de la Toile*) [18], [19] (travail en cours)

Note : Le nom utilisé pour ce protocole varie, désigné parfois comme le "Protocole de coordination des antémémoires de la Toile", mais fréquemment simplement "WCCP" pour éviter la confusion.

Description :
WCCP V1 fonctionne entre un routeur qui agit comme un élément de redirection du réseau et un mandataire d'interception hors chemin. Le protocole permet à un ou plusieurs mandataires de s'enregistrer auprès d'un seul routeur pour recevoir le trafic redirigé. Il permet aussi à un des mandataires, le mandataire désigné, d'imposer au routeur comment distribuer le trafic redirigé à travers le dispositif.

WCCP V2 fonctionne de plus entre plusieurs routeurs et les mandataires.

Sécurité :
WCCP V1 n'a pas de dispositifs de sécurité.
WCCP V2 fournit une authentification facultative des paquets de protocole.

Utilisation :
Éléments de réseau : WCCP est déployé sur une large gamme de routeurs Cisco.
Mandataires de mise en antémémoire : WCCP est déployé sur un certain nombre de mandataires de mise en antémémoire de divers fabricants.

Auteurs de la proposition :
David Forster
Les éditeurs du présent document.

8.2 Protocole de commande d'élément de réseau (NECP)

Meilleure référence connue :
"NECP: The Network Element Control Protocol" [22] (travail en cours)

Description :
NECP fournit des méthodes par lesquelles des éléments de réseau peuvent apprendre les capacités des serveurs, leur disponibilité, et avoir des indications sue les flux qui peuvent ou ne peuvent pas être servis. Cela permet aux éléments de réseau de faire de l'équilibrage de charge à travers un parc de serveurs, de la redirection sur des mandataires d'interception, et de court-circuiter les flux qui ne peuvent être servis par le parc.

Sécurité :
Utilise facultativement l'authentification par secret partagé HMAC-SHA-1 [11] avec des numéros de séquence complexes pour fournir une sécurité modérément forte. Le protocole est vulnérables aux attaques si l'authentification n'est pas utilisée.

Utilisation :
Inconnue pour l'instant ; plusieurs fabricants d'éléments de réseau et de mandataires d'antémémoire ont exprimé l'intention de mettre en œuvre le protocole.

Auteur de la proposition : Gary Tomlinson

8.3 SOCKS

Meilleure référence connue : RFC 1928 SOCKS Protocol Version 5 [7]

Description :
SOCKS est principalement utilisé comme mandataire d'antémémoire pour le protocole de pare-feu. Bien que les pare-feu ne se conforment pas à la définition stricte de l'élément de réseau donnée ci-dessus, il font partie intégrante de

l'infrastructure du réseau. Lorsque il est utilisé en conjonction avec un pare-feu, SOCKS fournit un tunnel authentifié entre le mandataire d'antémémoire et le pare-feu.

Sécurité :
Un cadre extensible permet de nombreuses méthodes d'authentification. Actuellement, SSL, CHAP, DES, 3DES sont disponibles.

Utilisation : SOCKS est largement déployé sur l'Internet.

Auteur de la proposition : Les éditeurs du présent document.

9. Considérations pour la sécurité

Le présent document propose une taxonomie pour la mise en antémémoire et la duplication sur la Toile. Les pratiques recommandées, l'architecture et les protocoles ne sont pas décrits en détail.

Par définition, la duplication et la mise en antémémoire impliquent la copie des ressources. Il y a des conséquences juridiques à la copie et la conservation de copies transitoires ou permanentes ; elle ne sont pas traitées dans ce document.

Les informations sur la sécurité de chaque protocole mentionné dans le présent mémoire sont données dans les sections précédentes, et dans la documentation qui les accompagne. La sécurité de HTTP est discutée dans la section 15 de la RFC 2616 [1], spécification de HTTP/1.1, et dans une moindre mesure dans la RFC 1945 [6], spécification de HTTP/1.0. La RFC 2616 contient les considérations sur la sécurité pour les mandataires HTTP.

Les mandataires de mise en antémémoire ont les mêmes problèmes de sécurité que les autres mandataires de niveau application. Les mandataires de niveau application ne sont pas traités dans les présentes considérations pour la sécurité. L'authentification fondés sur le numéro IP est problématique lorsque un mandataire est impliqué dans la communication. Les détails ne sont pas exposés ici.

9.1 Authentification

Les demandes de ressources de la Toile, et les réponses à de telles demandes, peuvent être dirigées sur des répliques et/ou peuvent s'écouler à travers des mandataires intermédiaires. L'intégrité des communications doit être préservée pour assurer la protection à la fois contre la perte d'accès et contre des changements non intentionnels.

9.1.1 Attaque par interposition *(Man in the middle)*

Les mandataires HTTP sont interposés, l'endroit idéal pour une attaque par interposition. Un exposé sur cette question se trouve à la section 15 de la RFC 2616 [1].

9.1.2 Tiers de confiance *(trusted third party)*

Un mandataire peut être de confiance pour agir au nom du serveur d'origine et/ou du client, ou il doit agir comme un tunnel. Lors de la présentation d'objets placés en antémémoire aux clients, celui-ci a besoin de faire confiance au mandataire de mise en antémémoire comme agissant au nom du serveur d'origine.

Une réplique peut obtenir une accréditation de la part du serveur d'origine.

9.1.3 Authentification fondée sur le numéro IP

L'authentification fondée sur le numéro IP du client pose problème lors de connexion à travers un mandataire, car l'appareil d'authentification n'a accès qu'au numéro IP du mandataire. Une solution (problématique) à cela est que le mandataire se fasse passer pour le numéro IP du client pour les demandes entrantes.

L'authentification fondée sur les numéros IP suppose que les propriétés de bout en bout de l'Internet sont préservées. Cela n'est typiquement pas le cas dans les environnements qui contiennent des mandataires d'interception.

9.2 Confidentialité

9.2.1 Tiers de confiance

Lors de l'utilisation d'un service de duplication, on doit faire confiance à la fois à la réplique de serveur d'origine et à la réplique du système de sélection.

La redirection du trafic – que ce soit par des méthodes de sélection automatique de réplique ou au sein de mandataires - peut introduire des tiers auxquels l'utilisateur final et/ou le serveur d'origine ne font pas confiance. Dans le cas des mandataires d'interception, de tels tiers sont souvent inconnus des deux points d'extrémité de la communication. Des tiers inconnus peuvent avoir des implications pour la sécurité.

Les mandataires et les services de sélection de réplique peuvent tous deux avoir accès à des informations d'accès agrégées. Un mandataires connaît normalement les accès de chaque client qui l'utilise, informations qui sont plus sensibles que celles qui sont détenues par un seul serveur d'origine.

9.2.2 Journaux d'enregistrement et implications juridiques

Les journaux d'enregistrement des mandataires devraient être conservés en sécurité, dans la mesure où ils fournissent des informations sur les utilisateurs et leurs schémas de comportement. Le journal d'enregistrement d'un mandataire est encore plus sensible qu'un journal d'enregistrement d'un serveur de la Toile, car toute demande de la population utilisatrice passe à travers le mandataire. Les journaux d'enregistrement des répliques de serveurs d'origine peuvent devoir être amalgamés pour obtenir des statistiques agrégées d'un service, et le transport de journaux d'enregistrement à travers des frontières peut avoir des implications juridiques. Le traitement des journaux d'enregistrement est interdit pas la loi dans certains pays.

Les exigences pour la sécurité des objets et pour la confidentialité sont les mêmes dans une réplique de la Toile ou dans un système de mise en antémémoire que sur le reste de l'Internet au sens large. La seule solution fiable est une cryptographie forte. Le chiffrement de bout en bout rend fréquemment les ressources inaccessibles, comme c'est le cas des sessions chiffrées avec SSL.

9.3 Sécurité du service

9.3.1 Déni de service

Toute redirection du trafic est susceptible d'attaques de déni de service au point de redirection, et les deux services de mandataires et de sélection de répliques peuvent rediriger le trafic.

En attaquant un mandataire, l'accès à tous les serveurs peut être dénié pour un gros ensemble de clients.

Il a été avancé que l'introduction d'un mandataire d'interception est une attaque de déni de service, car la nature de bout en bout de l'Internet est détruite sans que le consommateur du contenu le sache.

9.3.2 Attaque en répétition

Une antémémoire mandataire est par définition une attaque en répétition.

9.3.3 Configuration stupide de mandataire

Il est assez facile d'avoir une configuration stupide qui va endommager le service pour les consommateur de contenu. C'est le problème de sécurité le plus courant avec les mandataires.

9.3.4 Copies transitoires protégées par copyright

Les forces législatives du monde entier se penchent sur la question des copies transitoires, comme celles conservées dans les systèmes de réplication et d'antémémoire, qui sont légales. Les implications légales de la réplication et de la mise en antémémoire sont soumises aux lois locales.

Les antémémoires mandataires ont besoin de préserver les sorties de protocole, y compris les en-têtes. Les services de réplication ont besoin de préserver la source des objets.

9.3.5 Accès au niveau application

Les antémémoires mandataires sont des composants de niveau application dans le chemin du flux de trafic, et peuvent donner à des intrus l'accès aux informations qui n'étaient auparavant accessibles qu'au niveau réseau dans un monde sans mandataires. Certains équipements de niveau réseau peuvent exiger un accès physique pour obtenir des informations sensibles. L'introduction de composants de niveau application peut exiger des sécurités système supplémentaires.

10. Remerciements

Les éditeurs tiennent à remercier de leur assistance les personnes suivantes : David Forster, Alex Rousskov, Josh Cohen, John Martin, John Dilley, Ivan Lovric, Joe Touch, Henrik Nordstrom, Patrick McManus, Duane Wessels, Wojtek Sylwestrzak, Ted Hardie, Misha Rabinovich, Larry Masinter, Keith Moore, Roy Fielding, Patrik Faltstrom, Hilarie Orman, Mark Nottingham et Oskar Batuner.

Références

[1] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach et T. Berners-Lee, "Protocole de transfert Hypertexte -- HTTP/1.1", RFC 2616, juin 1999. *(D.S., MàJ par 2817)*

[2] D. Wessels, K. Claffy, "Protocole des antémémoires de l'Internet (ICP), version 2", RFC 2186, septembre 1997. *(Info.)*

[3] D. Wessels, K. Claffy, "Application du protocole des antémémoires de l'Internet (ICP), version 2", RFC 2187, septembre 1997. *(Information)*

[4] J. Postel et J. Reynolds, "Protocole de transfert de fichiers (FTP)", STD 9, RFC 959, octobre 1985.

[5] F. Anklesaria, M. Cahill, P. Lindner, D. Johnson, D. Torrey et B. Albert, "Protocole Gopher Internet (un protocole de recherche et restitution de documents répartis", RFC 1436, mars 1993. *(Information)*

[6] T. Berners-Lee, R. Fielding, H. Frystyk, "Protocole de transfert Hypertext -- HTTP/1.0**"**, RFC 1945, mai 1996. *(Info.)*

[7] M. Leech, M. Ganis, Y. Lee, R. Kuris, D. Koblas et L. Jones, "Protocole SOCKS version 5", RFC 1928, mars 1996.

[8] T. Brisco, "Prise en charge de l'équilibrage de charge par le DNS", RFC 1794, avril 1995. *(Information)*

[9] P. Vixie, D. Wessels, "Protocole de mise en antémémoire d'HyperTexte **(**HTCP/0.0)", RFC 2756, janvier 2000. *(Exp.)*

[10] Fan, L., Cao, P., Almeida, J. and A. Broder, "Summary Cache: A Scalable Wide-Area Web Cache Sharing Protocol", Proceedings of ACM SIGCOMM'98 pp. 254-265, septembre 1998.

[11] H. Krawczyk, M. Bellare et R. Canetti, "HMAC : Hachage de clés pour l'authentification de message", RFC 2104, février 1997.

[12] Netscape, Inc., "Navigator Proxy Auto-Config File Format", mars 1996, <URL:http://www.netscape.com/eng/mozilla/2.0/relnotes/demo/proxy-live.html>.

[13] P. Gauthier, J. Cohen, M. Dunsmuir et C. Perkins, "Protocole d'auto découverte de mandataire de la Toile", Travail en cours.

[14] V. Valloppillil et K. Ross, "Protocole d'acheminement à dispositif d'antémémoire", Travail en cours.

[15] Microsoft Corporation, "Cache Array Routing Protocol (CARP) v1.0 Specifications, Technical Whitepaper", août 1999, <URL:http://www.microsoft.com/Proxy/Guide/carpspec.asp>.

[16] Microsoft Corporation, "Cache Array Routing Protocol and Microsoft Proxy Server 2.0, Technical White Paper", août 1998, <URL:http://www.microsoft.com/proxy/documents/CarpWP.exe>.

[17] L. Lovric, "Internet Cache Protocol Extension", Travail en cours.

[18] M. Cieslak e D. Forster, "Cisco Web Cache Coordination Protocol V1.0", Travail en cours.

[19] M. Cieslak, D. Forster, G. Tiwana et R. Wilson, "Cisco Web Cache Coordination Protocol V2.0", Travail en cours.

[20] C. Goutard, I. Lovric et E. Maschio-Esposito, "Pre-filling a cache - A satellite overview", Travail en cours.

[21] Hamilton, M., Rousskov, A. and D. Wessels, "Cache Digest specification - version 5", décembre 1998, <URL:http://www.squid-cache.org/CacheDigest/cache-digest-v5.txt>.

[22] A. Cerpa, J. Elson, H. Beheshti, A. Chankhunthod, P. Danzig, R. Jalan, C. Neerdaels, T. Shroeder et G. Tomlinson, "NECP: The Network Element Control Protocol", Travail en cours.

[23] I. Cooper, J. Dilley, "Problèmes connus de mandataire/antémémoire dans HTTP", RFC3143, juin 2001. *(Information)*

Adresse des auteurs

Ian Cooper
Equinix, Inc.
2450 Bayshore Parkway
Mountain View, CA 94043
USA
téléphone : +1 650 316 6065
mél : icooper@equinix.com

Ingrid Melve
UNINETT
Tempeveien 22
Trondheim N-7465
Norway
téléphone : +47 73 55 79 07
mél : Ingrid.Melve@uninett.no

Gary Tomlinson
CacheFlow Inc.
12034 134th Ct. NE, Suite 201
Redmond, WA 98052
USA
téléphone : +1 425 820 3009
mél l: gary.tomlinson@cacheflow.com

Déclaration de copyright

Remerciement

Le financement de la fonction d'édition des RFC est actuellement fourni par l'Internet Society.