

①②

DEMANDE DE BREVET D'INVENTION

A1

②② Date de dépôt : 12.04.02.

③⑦ Priorité :

④③ Date de mise à la disposition du public de la
demande : 17.10.03 Bulletin 03/42.

⑤⑥ Liste des documents cités dans le rapport de
recherche préliminaire : *Ce dernier n'a pas été
établi à la date de publication de la demande.*

⑥⑦ Références à d'autres documents nationaux
apparentés :

⑦① Demandeur(s) : GOUGET MICHEL — FR.

⑦② Inventeur(s) : GOUGET MICHEL.

⑦③ Titulaire(s) :

⑦④ Mandataire(s) :

⑤④ PROCÉDE D'ETABLISSEMENT ET DE DEROULEMENT D'UNE LIAISON INFORMATIQUE.

⑤⑦ Procédé d'établissement et de déroulement d'une
liaison informatique.

La liaison relie un client et un serveur. Elle utilise les pro-
tocolos de l'Internet, et est déclenchée logiquement à la de-
mande du serveur. Le procédé permet d'éviter que le client
accepte des connexions entrantes. Il peut être utilisé notam-
ment lors d'opérations de télémaintenance, télé-transfert et
prise de main à distance sur de sites éloignés.

FR 2 838 593 - A1



Il est fréquent d'avoir de multiples installations informatiques (appelées par la suite « sites clients ») physiquement dispersées, pouvant être de types et natures variées et appartenir à des entités administratives différentes, et qui doivent être accédées à partir d'un ou quelques sites informatiques centraux. Ceci se produit en particulier lors de l'installation ou de la mise à jour de logiciels, de transfert de fichiers, de correction de dysfonctionnements, et plus généralement lors de toutes opérations d'administration, maintenance, exploitation, prise de main à distance, ou autres sur les sites clients. Une opération de ce type est appelée par la suite téléintervention. Habituellement la compétence informatique est faible sur les sites clients, au moins dans le domaine concerné par l'intervention, et intervenir à distance permet en particulier de mutualiser la compétence informatique rare et chère d'opérateurs qualifiés, diminuer les coûts et/ou procurer un meilleur service.

On rencontre en particulier cette situation dans le cas de SSII et vendeurs informatiques devant fournir support et assistance à un parc installé.

Les accès au site client doivent être sécurisés, afin en particulier d'éviter les intrusions, offrir un débit de données adapté aux opérations à effectuer pour notamment fournir un bon confort d'utilisation, être fiables et disponibles (intervention possible à toute heure, caractère d'urgence...), ne pas nécessiter d'intervention du personnel des sites clients, être d'une installation et d'une mise en œuvre facile et souple y compris dans des environnements informatiques hétérogènes, et être économiques, particulièrement lors de la mise en œuvre et l'exploitation, spécialement dans le cas d'interventions longues ou sur des sites géographiquement éloignés.

Il n'existe pas actuellement de procédé d'accès satisfaisant pleinement ces contraintes.

A titre d'exemple, un réseau privé d'entreprise n'est pas utilisable pour des entreprises multiples; les réseaux virtuels privés proposés par des compagnies de télécommunication sont chers; laisser sur chaque site client une machine disposant d'un accès entrant ouvert depuis l'Internet est très dangereux sans une excellente compétence informatique locale pour le protéger et éviter les intrusions, etc.

En pratique, la majorité des systèmes de téléintervention utilisent le réseau téléphonique standard, avec des modems, et parfois un encryptage, des mots de passe et/ou un rappel automatique. Cette solution présente de nombreux désavantages, en particulier un débit de données limité et non adaptable, une liaison peu fiable tant lors de l'établissement que dans la durée, un temps d'établissement important, une sécurité aléatoire et un coût important.

Le procédé objet de l'invention permet de réaliser de tels accès sans les inconvénients indiqués. Il permet de raccorder d'une manière raisonnablement sécurisée les sites clients à l'Internet tout en permettant aux sites centraux d'y accéder.

Pour cela, le site client comporte au moins une machine (le client) disposant d'un accès au moins sortant (direct ou via pare-feu, etc.) et le site central comporte une machine (le serveur) disposant d'un accès au moins entrant sur l'Internet ou un réseau ou environnement utilisant le protocole TCP/IP. On appelle unité d'exécution un objet exécutant une suite d'instructions sur une machine; cela correspond, selon les environnements, à un processus, une tâche, un thread, un démon, etc. À l'initiative du client (au démarrage par exemple), une unité d'exécution cliente établit une connexion selon les protocoles de l'Internet vers une unité d'exécution située sur le serveur, crée un canal de communication bidirectionnel (appelé par la suite socket) entre les deux, et envoie une flux de données simulant une question. Les deux unités d'exécution peuvent être physiquement sur le même site ou la même machine. Ainsi, vu du réseau et des systèmes de sécurité du site client, on a affaire à une communication sortante habituelle. Tant que le site central ne désire pas se connecter, le serveur ne répond pas, ou peut aussi renvoyer périodiquement ou non des données de remplissage pour garder le socket ouvert. Si, pour une raison quelconque, par exemple à cause d'une trop grande période d'inactivité, le socket se ferme, le client peut en recréer un nouveau de manière identique ; dans ce cas, à réception de cet appel entrant du même client, le serveur peut fermer l'ancien, et considérer le nouveau comme étant le socket actif. Quand le site central désire se connecter, le serveur répond en envoyant la requête désirée sur le socket actif, en l'habillant pour qu'elle devienne, vu de l'extérieur, la charge utile de la réponse à la requête du site client. Le client répond à cette question par une réponse habillée pour être la charge utile d'une question au sens du protocole utilisé. La suite du dialogue s'effectue soit par l'intermédiaire dudit socket resté ouvert, soit grâce à de nouveaux sockets créés de manière similaire par le client, soit par un mélange de ces méthodes. Suivant les modes de réalisation et les protocoles utilisés, certaines questions, tant réelles que au sens du protocole utilisé peuvent comporter aucune ou plusieurs réponses, et certaines questions et réponses au sens du protocole utilisé peuvent ne pas être utilisées et ne servir que de remplissage par exemple.

On réalise ainsi une connexion créée physiquement à l'initiative du site client, mais logiquement à l'initiative du site central, dans laquelle transite des questions au sens du protocole utilisé émises par le client, dont au moins certaines comportent dans leur charge utile des réponses à des questions logées dans la charge utile de réponses au sens du protocole utilisé émises par le serveur.

La première question au sens du protocole utilisé émise par le client peut comporter dans sa charge utile des informations sur l'état de l'unité d'exécution cliente et son environnement.

Par ailleurs, le client peut initialiser autant de liaisons que nécessaire à des moments judicieusement choisis (par exemple et à titre non limitatif lors de la première réception de données en provenance du serveur) de sorte qu'il y ait toujours une liaison disponible.

Procéder ainsi permet notamment au site client d'interdire (via un pare-feu par exemple) toute connexion entrante sans impacter le fonctionnement du procédé, ce qui est un avantage de sécurité très important car on supprime ainsi la grande majorité des possibilités d'intrusion. Cela évite aussi toute les contraintes d'adressage, routage et résolution de noms liés à la réalisation d'une connexion entrante.

Le site central accepte les communications entrantes, mais cela ne pose pas de problèmes de sécurité cruciaux car, en général le site central dispose de compétences informatiques pour effectuer un paramétrage correct, et de plus, il est beaucoup plus facile de sécuriser un seul site qu'une multitude.

Ce procédé est très économique car, contrairement au téléphone par exemple, les connexions TCP/IP ne sont habituellement tarifées ni à la durée, ni au volume, ni à la distance, ni au nombre de liaisons actives mais selon la bande passante disponible de la liaison. Lorsque aucune opération de téléintervention n'est en cours, la totalité de cette bande passante est disponible pour d'autres usages (typiquement courrier électronique et accès à la toile mondiale); en cas d'activité, la bande passante est facilement partagée sans opération particulière à effectuer. De plus, très fréquemment, une liaison Internet permanente existe déjà sur le site client, et peut être utilisée par le système de téléintervention, supprimant ainsi tous investissements et dépenses télécoms supplémentaires liées à la téléintervention.

Ce procédé procure un bien meilleur confort d'utilisation que le téléphone, car, contrairement à ce dernier, les liaisons Internet sont en général permanentes, et de plus disponibles en de multiples classes de débit, permettant ainsi un ajustement souple et facile aux besoins. De plus, ces types de liaisons sont identiques au niveau mondial sans variantes ni licences spécifiques locales, contrairement aux réseaux de type téléphone ou RNIS.

Il est possible d'utiliser tout protocole sur le socket, donc en particulier des protocoles standards comme par exemple HTTP, HTTPS ou SOAP. Procéder ainsi permet en particulier au client grâce à l'utilisation de syntaxes, protocoles et/ou adresses judicieuses de générer des liaisons similaires à celles effectuées habituellement par le site client, et donc difficilement discernables de celles-ci, tout du moins par les dispositifs de sécurité locaux. Par exemple, il est possible de simuler le comportement d'un utilisateur ordinaire connecté à l'Internet via son poste de travail, type de connexion quasiment toujours autorisé par les dispositifs de protection (pare feux par exemple) et le réseau informatique du site client. Ainsi, aucune modification desdits dispositifs n'est nécessaire lors de l'installation sur le site client.

De même, les connexions peuvent être authentifiées et encryptées, grâce par exemple à l'utilisation de protocoles et algorithmes à clé publique ou privée, et/ou de certificats, et/ou de tiers certificateurs, et/ou de signatures numériques.

Les connexions peuvent aussi encapsuler tout autre protocole, permettant ainsi en particulier dans la charge utile le multiplexage (cas du protocole PPP par exemple) de plusieurs flux d'informations entrants et/ou sortants, et/ou la réalisation de passerelles entre programmes, et/ou la transmission d'informations de toute nature (par exemple audio ou vidéo) entre les sites.

5 De même les unités d'exécution client et/ou serveur peuvent jouer un rôle d'aiguilleurs en routant et/ou multiplexant/démultiplexant les requêtes et/ou données reçues vers et/ou depuis un opérateur et/ou des dispositifs quelconques (à titre non limitatif : caméras, microphones, capteurs, actionneurs, systèmes d'acquisition/restitution du son, de l'image ou de la vidéo...) et/ou autres unités de traitement et/ou autres systèmes, et en renvoyant les réponses vers ceux-ci.

10 La liaison peut aussi ne pas être permanente. Dans ce cas, le client a toute latitude pour établir la liaison, par exemple selon des tranches horaires ou la survenance de tout type d'évènements (alarmes, dysfonctionnements...), ou demande d'un opérateur du site client.

Il est possible de redonder les connexions et/ou unités d'exécution, coté client et/ou serveur, afin de se prémunir d'éventuels dysfonctionnements et améliorer la disponibilité de l'ensemble.

15 Dans ce cas, selon un mode préférentiel d'exécution de l'invention, l'ensemble est judicieusement agencé de manière qu'en cas d'unité et/ou de connexion défailante, une autre unité et/ou une autre connexion prenne le relais, afin de maintenir et/ou rétablir la liaison.

Un exemple non limitatif de mise en œuvre de l'invention est représenté sur la figure 1). Le site
20 client comprend la machine cliente (1) connectée au réseau Internet (11) via un routeur et un pare-feu non représentés empêchant toute connexion entrante, sur lequel tourne un démon (2) activé au démarrage de la machine, supportant les protocoles SOAP et HTTP. L'opérateur (9) accède au site central via un logiciel de navigation (browser WEB) standard en utilisant les protocoles HTTP et HTML, à travers le réseau Internet (11). Le site central se compose d'un
25 serveur (10) fonctionnant sous système d'exploitation multitâches connecté au réseau Internet (11) via un routeur et un pare-feu non représentés. Sur ce serveur fonctionne un serveur WEB standard (4), l'ensemble étant paramétré de sorte qu'un processus (5) soit exécuté à réception d'une requête SOAP reçue sur l'URL (3) émis par le démon (2) et que le processus (7) soit exécuté à réception d'une requête HTML reçue sur l'URL (8) envoyée par l'opérateur (9), grâce
30 à une interface CGI par exemple. Un démon (6) est activé sur (10) au démarrage, auquel peuvent se connecter les processus (5) et (7) par un mécanisme à base de sockets par exemple. Les étapes des échanges et actions des différents composants sont les suivantes :

- Etape 1) : Au démarrage, (2) envoie une requête vide SOAP (X) sur l'URL (3) géré par le serveur WEB (4), ce qui active (5) qui se connecte à (6) via un socket, transmet la requête et
35 attend une réponse sur celui-ci. Le résultat de cette action est que (6) note dans ses tables internes les coordonnées de (2)

- Etape 2) : Quelque temps après (9) envoie une requête HTML réelle (Y) sur l'URL (8) géré par (4), ce qui active (7) qui se connecte à (6) via un socket, transmet la requête et attend une réponse sur celui-ci.
- 5 • Etape 3) : (6) code et met en forme cette requête HTML afin qu'elle soit syntaxiquement vue comme la réponse à la requête SOAP (X), et renvoie le résultat à (5), qui le transmet au serveur WEB (4) qui lui-même le retransmet à (2).
- Etape 4) : (2) reçoit cette pseudo réponse SOAP, qui est en réalité la question contenue dans la requête HTML (Y), calcule la réponse à cette question, la code et la met en forme afin qu'elle soit syntaxiquement vue comme une requête SOAP (Z), et renvoie ce résultat sur
10 l'URL (3) géré par (4), ce qui active (5) qui le transmet à (6). (2) est alors dans le même état qu'à la fin de l'étape 1).
- Etape 5) : (6) décode et met en forme cette pseudo requête afin de fabriquer une réponse HTML qui est transmise à (4) qui la retourne à l'opérateur (9) en tant que réponse à la requête HTML (Y).
- 15 Les étapes 2) à 5) peuvent être répétées indéfiniment. Les processus (4), (5), (6), et (7) peuvent être implémentés de manière séparée ou non selon les environnements informatiques.
- Concernant les étapes 1) à 5) : Vu de l'opérateur, (9) a envoyé une question HTML à (1), et reçu peu de temps après une réponse HTML. Vu du serveur WEB, (1) a envoyé une requête SOAP à (10), a reçu une réponse SOAP peu de temps après, puis a renvoyé une autre requête SOAP qui
20 est en attente de réponse. Vu de l'Internet, (1) n'a reçu aucun appel entrant ni requête et en a émis deux. On réalise donc l'objet de l'invention, c'est à dire une communication physiquement à l'initiative du client, mais logiquement à l'initiative du serveur.

25 Ce procédé peut être utilisé en particulier dans les logiciels, solutions et systèmes de télémaintenance, télé exploitation, transfert de fichiers, télé-administration, télésurveillance, télédiffusion ou télé-collecte de fichiers, logiciels ou autres, télé-mise-à-jour de sites, applications ou autres, consolidation d'informations et/ou de données.

REVENDICATIONS

- 1) Procédé d'établissement et de déroulement d'une liaison informatique selon les protocoles de l'Internet entre une unité d'exécution cliente située sur un site client et une unité d'exécution serveur située sur un site serveur, lesdites unités pouvant être physiquement sur le même site
5 et/ou la même machine, caractérisé en ce que l'unité cliente établit la connexion vers l'unité serveur, que l'unité cliente envoie au sens du protocole utilisé des questions et reçoit au sens du protocole utilisé zéro ou plusieurs réponses à chaque question, et que la charge utile de certaines réponses au moins est en réalité une question de l'unité serveur, et la charge utile de certaines questions au moins est en réalité une réponse à une question de l'unité serveur, la première
10 question au sens du protocole utilisé émise par l'unité cliente servant de remplissage pour respecter le protocole utilisé.
- 2) Procédé selon la revendication précédente, caractérisé en ce qu'il est utilisé dans des logiciels, solutions et systèmes de télémaintenance, téléexploitation, transfert de fichiers, télé-administration, télésurveillance, télédiffusion ou télé-collecte de fichiers, logiciels ou autres,
15 télé-mise-à-jour de sites, applications ou autres, consolidation d'informations et/ou de données.
- 3) Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que la charge utile de la première question au sens du protocole utilisé émise par l'unité cliente contient en réalité au moins partiellement des informations sur l'état de l'unité d'exécution cliente et de son environnement.
- 20 4) Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que l'unité cliente initialise plusieurs liaisons à des moments judicieusement choisis de sorte qu'il y en ait toujours au moins une disponible.
- 5) Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que les protocoles et/ou la syntaxe et/ou les adresses utilisés rendent la liaison similaire aux autres
25 liaisons s'effectuant habituellement sur le site client et/ou difficilement discernable de celles-ci.
- 6) Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que tout ou partie des données entrantes et/ou sortantes est encrypté et/ou authentifié et/ou signé numériquement.
- 7) Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que les
30 charges utiles des questions et/ou des réponses au sens du protocole utilisé sont organisées de manière à multiplexer plusieurs flux d'information entrants et/ou sortants.
- 8) Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que l'unité de traitement serveur et/ou l'unité de traitement client effectue un routage et/ou un multiplexage/démultiplexage de données en provenance et/ou à destination de dispositifs et/ou
35 systèmes et/ou unités de traitement et/ou opérateurs humains.

- 9) Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il existe des unités de traitement supplémentaires sur le site client et/ou le site serveur, et/ou qu'il existe plusieurs possibilités de connexion entre lesdites unités, et que l'ensemble est agencé de sorte qu'en cas d'unité et/ou de connexion défaillante, une autre unité et/ou une autre connexion prenne le relais afin de maintenir et/ou rétablir la liaison.
- 5

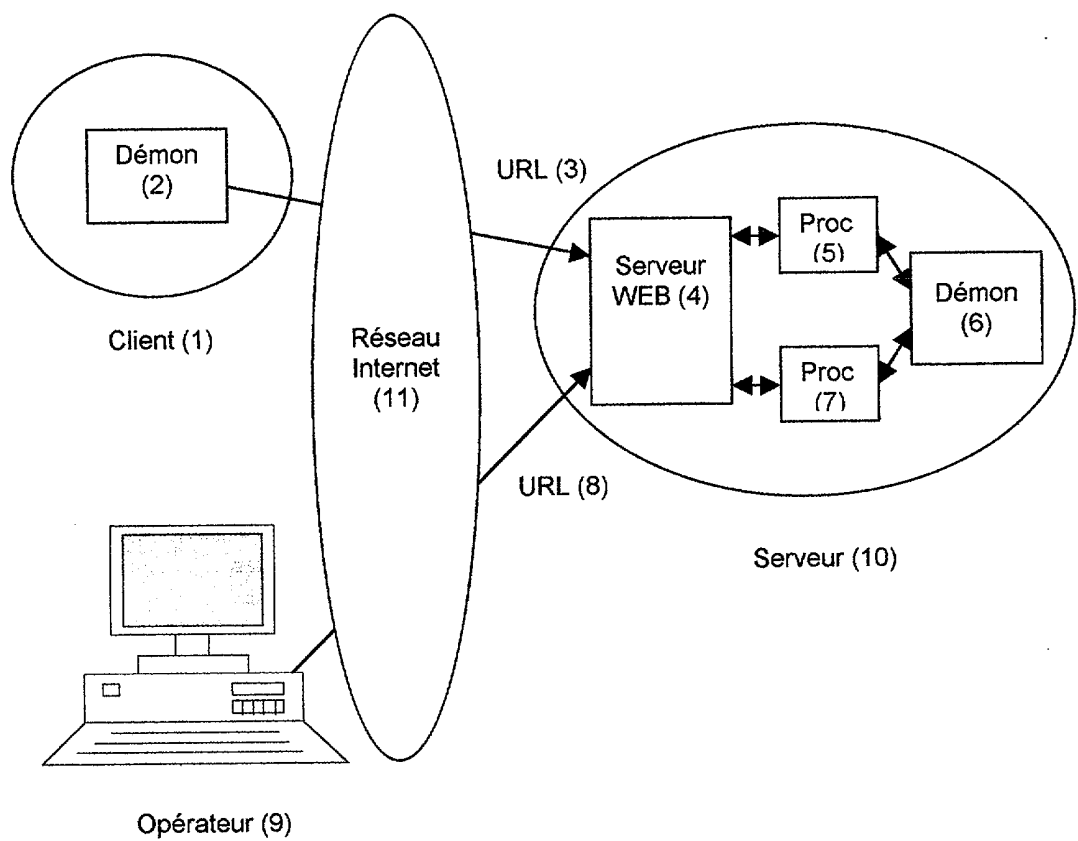


FIG. 1