(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** ***3 093 258***

(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **19 01975**

(51) Int Cl[8] : ***H 04 L 12/26*** *(2019.01), G 06 F 21/57*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 26.02.19.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 28.08.20 Bulletin 20/35.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

( ) **Demande(s) d'extension :**

(71) **Demandeur(s) :** *ALSID Société par actions simplifiée* — FR.

(72) **Inventeur(s) :** COLTEL Romain et DELSALLE Luc.

(73) **Titulaire(s) :** ALSID Société par actions simplifiée.

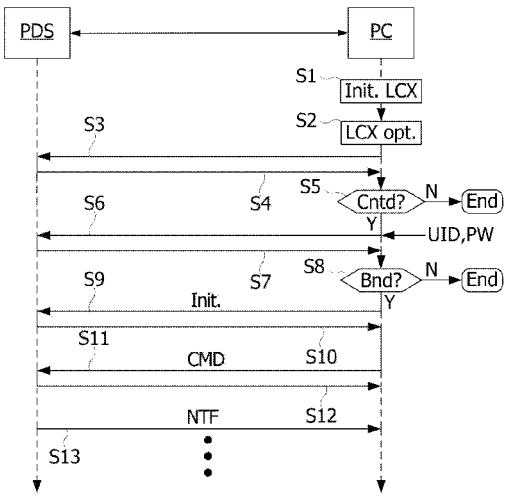
(74) **Mandataire(s) :** OMNIPAT.

(54) PROCEDE DE PROTECTION D'UN RESEAU PRIVE D'ORDINATEURS.

(57) PROCEDE DE PROTECTION D'UN RESEAU PRIVE D'ORDINATEURS

L'invention concerne un procédé de collecte de données d'un service d'annuaire utilisé pour administrer un réseau privé comprenant un ensemble d'ordinateurs (PDS,PC) interconnectés, le service d'annuaire rassemblant des données relatives à des objets du réseau, le procédé comprenant des étapes consistant à : connecter un terminal (PC) à un serveur du réseau (PDS) comprenant une instance du service d'annuaire, configurer l'instance du service d'annuaire sur le serveur par le terminal, pour que le terminal soit notifié de modifications apportées aux données du service d'annuaire, recevoir par le terminal des messages de notification (NTF) contenant des données modifiées du service d'annuaire, transmis par le serveur, et traiter chacun des messages de notification reçu pour déterminer les modifications apportées aux données du service d'annuaire.

Figure pour l'abrégé : Fig. 3



FR 3 093 258 - A1

Description

Titre de l'invention : PROCEDE DE PROTECTION D'UN RESEAU PRIVE D'ORDINATEURS

[0001] La présente invention concerne la protection d'un réseau privé d'ordinateurs interconnectés. La présente invention vise notamment à superviser la sécurité d'un réseau privé de serveurs interconnectés par l'intermédiaire de réseaux de transmission de données privés ou publics, les outils de gestion relatifs à un tel ensemble étant rassemblées dans un service d'annuaire (directory service) utilisant une base de données pour y stocker toutes les données nécessaires. La présente invention s'applique notamment aux services d'annuaire Microsoft™ Active Directory, et Samba.

[0002] Un service d'annuaire de ce type vise à fournir des services centralisés de gestion d'un réseau privé d'ordinateurs, ainsi que des services d'identification et d'authentification permettant notamment d'accéder au réseau privé. Elle permet également d'autoriser l'installation de mises à jour critiques par des administrateurs désignés, de répertorier les éléments et ressources du réseau, tels que les comptes des utilisateurs, les serveurs, les postes de travail, les dossiers partagés, les imprimantes, etc. Un utilisateur du réseau privé peut ainsi facilement trouver des ressources partagées, et les administrateurs peuvent contrôler leur utilisation grâce à des fonctionnalités de distribution, de duplication, de partitionnement et de sécurisation de l'accès aux ressources répertoriées. Toutes les informations nécessaires à la fourniture de ces services dans des conditions de sécurité appropriées sont rassemblées dans une base de données distribuée sur un ou plusieurs serveurs du réseau privé appelés "contrôleurs de domaine". Chaque contrôleur d'un même domaine stocke localement une copie de la base de données qui peut rassembler quelques centaines à plusieurs millions d'objets pour les très grands réseaux privés d'ordinateurs.

[0003] La base de données d'un service d'annuaire de type "Active Directory" présente une structure hiérarchique rassemblant des informations sur des objets notamment de type ressource, service, utilisateur ou groupe d'utilisateurs. Un objet est identifié de manière unique par un identifiant et est associé à un ensemble d'attributs définissant les caractéristiques et informations que l'objet peut contenir. La structure de chacun des objets mémorisés dans la base de données est définie par un objet de type schéma.

[0004] Par ailleurs, pour assurer la cohérence des copies locales de la base de données, stockées par les différents contrôleurs de domaine du réseau privé, le service d'annuaire comprend des mécanismes de réplication assurant la transmission et la propagation des modifications effectuées dans une copie locale de la base de données vers les autres copies locales stockées dans le réseau privé. Cette propagation est réalisée

selon une topologie de réplication où chaque contrôleur de domaine peut être le siège de modifications (ajout, modification, suppression) de la base données.

[0005] La protection d'un réseau privé d'ordinateurs mettant en œuvre un service d'annuaire de type "Active Directory" est généralement assurée en amont par un ajustement adéquat de paramètres de sécurité, et en aval par l'analyse de journaux d'événements produits par les contrôleurs de domaine. Une telle analyse requiert l'activation de services de journalisation avancés sur les contrôleurs de domaine, et la mise en place d'un redirecteur d'événements assurant la transmission des informations à analyser vers un point central de collecte (un ordinateur du réseau) où l'analyse des événements est effectuée. En effet, de nombreuses violations de la sécurité d'un réseau privé peuvent être détectées dès l'apparition de l'événement si le journal d'événement approprié est activé, l'absence d'analyse de tels journaux apparaît comme une faille de sécurité pour de nombreux réseaux privés. Cependant, il s'avère que le volume d'informations relatives à la sécurité rapporté au volume total d'informations recueillies dans ces journaux est extrêmement déséquilibré et donc peu adapté à la mise en œuvre d'une analyse de sécurité efficace.

[0006] Une autre méthode de protection d'un service d'annuaire de type "Active Directory" couramment mise en œuvre, consiste à installer sur les contrôleurs de domaine des sondes logicielles configurées pour recueillir des informations sur les applications ou le système d'exploitation, exécutés par le contrôleur de domaine. Cependant, de telles sondes logicielles doivent agir au cœur du système d'exploitation du contrôleur de domaine. Elles peuvent donc entrainer des dysfonctionnements du système ou générer des failles de sécurité susceptibles d'être exploitées par d'éventuels attaquants.

[0007] Il est donc souhaitable de pouvoir proposer un procédé de protection d'un réseau d'ordinateurs, capable de détecter efficacement et d'une manière étendue, des failles de sécurité et des attaques, sans risque de perturber le fonctionnement ou d'affecter la sécurité d'un des contrôleurs de domaine du réseau.

[0008] Des modes de réalisation concernent un procédé de collecte de données d'un service d'annuaire utilisé pour administrer un réseau privé comprenant un ensemble d'ordinateurs interconnectés, le service d'annuaire rassemblant des données relatives à des objets du réseau, le procédé comprenant des étapes consistant à : connecter un terminal à un serveur du réseau comprenant une instance du service d'annuaire, configurer l'instance du service d'annuaire sur le serveur par le terminal, pour que le terminal soit notifié de modifications apportées aux données du service d'annuaire, recevoir par le terminal des messages de notification contenant des données modifiées du service d'annuaire, transmis par le serveur, et traiter chacun des messages de notification reçu pour déterminer les modifications apportées aux données du service d'annuaire.

[0009] Selon un mode de réalisation, le procédé comprend des étapes consistant à : télécharger, par le terminal, les données du service d'annuaire dans une copie locale gérée par le terminal, et à chaque réception d'un message de notification par le terminal, insérer dans la copie locale la valeur courante de la donnée modifiée indiquée dans le message de notification.

[0010] Selon un mode de réalisation, des données du service d'annuaire sont stockées dans une base de données gérée par le serveur, un des messages de notification contenant une nouvelle valeur d'une donnée du service d'annuaire, le procédé comprenant des étapes consistant à : comparer la donnée modifiée à une valeur précédente de la donnée modifiée mémorisée dans une copie locale gérée par le terminal, pour identifier un type de modification, et insérer la nouvelle valeur de la donnée modifiée dans la copie locale.

[0011] Selon un mode de réalisation, des données du service d'annuaire sont stockées dans des fichiers gérés par le serveur, un des messages de notification contenant une référence à un fichier modifié et un type de modification apportée au fichier, le procédé comprenant des étapes consistant à : télécharger par le terminal le fichier modifié indiqué dans le message de notification, comparer le fichier téléchargé à une version précédente du fichier modifié mémorisée dans une copie locale gérée par le terminal, pour identifier les données modifiées dans le fichier, et insérer le fichier téléchargé ou les données modifiées du fichier dans la copie locale.

[0012] Selon un mode de réalisation, le procédé comprend une étape de filtrage par le terminal des données du service d'annuaire reçues pour en extraire des données pertinentes pour détecter des anomalies, seules les données ainsi extraites étant stockées dans la copie locale.

[0013] Selon un mode de réalisation, le procédé comprend une étape de conversion des données de service d'annuaire reçues par le terminal en format alphanumérique ou en données structurées avant de les stocker dans la copie locale.

[0014] Des modes de réalisation peuvent concerner également un procédé de protection d'un réseau privé comprenant un ensemble d'ordinateurs interconnectés, le réseau étant administré par l'intermédiaire d'un service d'annuaire rassemblant des données de service d'annuaire relatives à des objets du réseau, le procédé comprenant des étapes consistant à : mettre en œuvre par un terminal le procédé de collecte de données de service d'annuaire tel que défini précédemment, pour acquérir des données d'une instance de service d'annuaire d'un serveur du réseau, gérant le service d'annuaire, stocker les données de service d'annuaire acquises dans une copie locale gérée par le terminal, à chaque fois qu'un message de notification de modification d'une donnée du service d'annuaire est reçue, analyser par le terminal, la donnée modifiée par rapport aux données de service d'annuaire stockées dans la copie locale, pour déterminer si

une modification appliquée aux données du service d'annuaire génère une faille de sécurité du réseau ou révèle une attaque du réseau, et générer un message d'alerte en cas de détection d'une faille de sécurité ou d'une attaque du réseau.

[0015] Selon un mode de réalisation, l'analyse de la donnée modifiée comprend des étapes consistant à : rechercher dans la copie locale une valeur précédente de la donnée modifiée, et comparer la valeur courante de la donnée modifiée à la valeur précédente de la donnée modifiée, un message d'alerte étant généré si la comparaison révèle l'apparition d'une faille de sécurité ou une attaque du réseau.

[0016] Selon un mode de réalisation, l'analyse d'une donnée modifiée comprend des étapes consistant à : rechercher dans la copie locale plusieurs valeurs précédentes de la donnée modifiée, et comparer entre elles la valeur courante de la donnée modifiée et les valeurs précédentes de la donnée modifiée, un message d'alerte étant généré si la comparaison révèle l'apparition d'une faille de sécurité ou une attaque du réseau.

[0017] Selon un mode de réalisation, l'analyse d'une donnée modifiée comprend des étapes consistant à : rechercher dans la copie locale la valeur d'au moins une donnée corrélée à la donnée modifiée, et déterminer si la valeur courante de la donnée modifiée considérée en corrélation avec la valeur de la donnée corrélée, révèle l'apparition d'une faille de sécurité ou une attaque du réseau.

[0018] Selon un mode de réalisation, les objets du réseau comprennent des serveurs, des terminaux d'utilisateurs, des appareils périphériques, des utilisateurs, des groupes d'utilisateurs, des services,

[0019] De modes de réalisation peuvent également concerner un terminal configuré pour mettre en œuvre l'un ou l'autre des procédés tels que définis précédemment.

[0020] De modes de réalisation peuvent également concerner un produit programme d'ordinateur directement chargeable dans une mémoire interne d'un ordinateur et comprenant des portions de code qui lorsqu'elles sont exécutées par un ordinateur configurent l'ordinateur pour mettre en œuvre l'un ou l'autre des procédés tels que définis précédemment.

[0021] Des exemples de réalisation de l'invention seront décrits dans ce qui suit, à titre non limitatif en relation avec les figures jointes parmi lesquelles :

[0022] [fig.1]

la figure 1 représente un exemple de réseau privé d'ordinateurs dans lequel le procédé de protection peut être mis en œuvre,

[0023] [fig.2]

la figure 2 représente schématiquement une architecture logicielle dans laquelle le procédé de protection est mis en œuvre, selon un mode de réalisation,

[0024] [fig.3]

la figure 3 illustre des étapes d'une procédure de recueil d'événements apparaissant

dans un service d'annuaire, selon un mode de réalisation,

[0025] [fig.4]

la figure 4 illustre des étapes d'une procédure de recueil d'événements apparaissant dans un service d'annuaire, selon un autre mode de réalisation.

[0026] La figure 1 représente un exemple de réseau privé d'ordinateurs dans lequel des procédés de collecte et de protection du réseau peuvent être mis en œuvre. Le réseau privé d'ordinateurs comprend un ou plusieurs domaines, chaque domaine comprenant un ou plusieurs serveurs DS1, DS2 configurés pour assurer la fonction de contrôleur de domaine, et éventuellement un ou plusieurs autres serveurs SV1, SV2, SV3 assurant par exemple la fonction de serveur de fichiers. Le réseau comprend également des terminaux P1-P7, des stations périphériques I1-I3, telles que des imprimantes, des scanners, etc., et un réseau local LN1, LN2 interconnectant les serveurs, les terminaux et les stations périphériques du domaine. Ici, le terme "terminal" peut désigner un ordinateur personnel, une station de travail, ou plus généralement, un équipement susceptible de se connecter au réseau local LN1, LN2, capable de communiquer avec l'un des serveurs DS1, DS2 pour émettre, requérir et recevoir des données, et traiter ces données.

[0027] Deux domaines du réseau privé peuvent être interconnectés par un réseau public PNT, chaque domaine étant connecté au réseau public par l'intermédiaire d'une passerelle ou d'un routeur M1, M2. Il est à noter qu'un même domaine peut comprendre plusieurs sous-réseaux locaux privés interconnectés par un réseau public. Chaque contrôleur de domaine DS1, DS2 du réseau met en œuvre un service d'annuaire pour assurer la gestion du domaine. Un tel service d'annuaire met en œuvre une base de données gérée grâce à un protocole d'accès aux annuaires tel que le protocole LDAP (Lightweight Directory Access Protocol). Une copie locale de la base de données peut être peut être stockée par chacun des différents contrôleurs de domaine DS1, DS2 du réseau. Dans le cas du service Microsoft™ Active Directory, chaque contrôleur de domaine DS1, DS2 du réseau stocke une copie locale de cette base de données, et des mécanismes de réplication sont mis en œuvre entre les contrôleurs de domaine pour assurer la cohérence entre les différentes copies locales de cette base de données.

[0028] La figure 2 représente une architecture de mise en œuvre des procédés de collecte et de protection, selon un mode de réalisation. La figure 2 représente des modules du service d'annuaire mis œuvre par un serveur PDS, et des modules mettant en œuvre les procédés de collecte et de protection, installés sur un terminal PC, connecté au serveur PDS, en tant qu'utilisateur du domaine contrôlé par le serveur PDS. Le serveur PDS peut être n'importe lequel des serveurs contrôleur de domaine DS1, DS2, et le terminal peut être n'importe lequel terminaux P1-P7.

[0029] Pour assurer le service d'annuaire, le serveur PDC comprend un module d'accès STE à une base de données ADDB du service d'annuaire, un module de gestion DAG du service d'annuaire et un module de communication serveur LDC mettant en œuvre un protocole d'accès à un service d'annuaire, tel que le protocole LDAP. Le module DAG organise et contrôle les accès à la base de données, notamment en fournissant à chacun des utilisateurs du réseau, un accès limité à une partie de la base de données ADDB, relative à une unique unité d'organisation à laquelle appartient l'utilisateur. Certains utilisateurs, appartenant à un groupe d'administrateurs disposent d'un accès complet à la base de données.

[0030] Dans le cas du service Microsoft™ Active Directory, le module STE est une bibliothèque logicielle rassemblant des fonctions de manipulation de bases de données selon la méthode séquentielle indexée, et mettant en œuvre des mécanismes permettant de réaliser des transactions atomiques, cohérentes, isolées et durables, ainsi que des mécanismes de mémoire cache, de verrou et de journalisation en vue d'assurer la sécurité et la performance des opérations effectuées sur la base de données ADDB.

[0031] La base de données ADDB présente une organisation hiérarchisée d'objets qui peuvent être classés en trois grandes catégories : les ressources (par exemple les imprimantes), les services (par exemple le courrier électronique) et les utilisateurs (comptes utilisateurs et groupes). Chaque objet de la base de données objet représente une entité unique (par exemple un utilisateur, un ordinateur, une imprimante ou un groupe), et regroupe, notamment sous la forme d'attributs, des informations sur l'objet. Certains de ces objets peuvent également être des conteneurs ou des éléments techniques complémentaires pour d'autres objets. Un objet est identifié de manière unique dans la base de données par son nom et possède son propre jeu d'attributs représentant les caractéristiques et les informations que l'objet peut contenir. La structure de chaque objet est définie par un schéma qui détermine également le type d'objet, les schémas des objets étant également stockés dans la base de données ADDB.

[0032] Le nombre de types d'objets disponibles dans la base de données ADDB n'est pas limité. Ainsi, la base de données ADDB peut contenir par exemple des objets des types suivants :

[0033] - unité d'organisation (conteneurs créant une hiérarchie d'objets au sein d'un domaine ; les unités d'organisation sont principalement utilisées pour permettre une délégation de droits et pour appliquer des stratégies de groupe à l'ensemble des objets de l'unité d'organisation,

[0034] - ordinateur (serveur, terminal, station de travail, ...),

[0035] - utilisateur,

[0036] - groupe (principalement utilisé pour établir des listes d'utilisateurs afin de leur attribuer un même ensemble de droits et/ou de services).

[0037] Selon un mode de réalisation, une application MNEG de surveillance du service d'annuaire est installée et exécutée par le terminal PC, cette application étant connectée et communiquant avec le serveur PDS via le réseau et le module LDC pour recevoir des événements de modifications apportés à la base de données ADDB. A cet effet, l'application de surveillance MNEG comprend un module de communication client CLD mettant en œuvre le protocole d'accès au service d'annuaire du server PDS (par exemple le protocole LDAP) pour communiquer avec le module LDC du serveur PDS, un module ACL de détection de changements dans la base de données ADDB exploitant les données reçues par le module CLD, un module de filtrage et de décodage DCF, un module de synchronisation SYF, un module d'analyse SAF, un module de stockage STF, et un module de communication MSGF permettant aux modules ACL, DCF, SYF, SAF et STF de communiquer entre eux.

[0038] Le module de communication client CLD met en œuvre un protocole d'accès au service d'annuaire du server PDS (par exemple LDAP), et configure une commande de recherche dans le service d'annuaire implémenté par les modules LDC et DAG, pour être notifié de toute modification du contenu de la base de données ADDB, pour recevoir ces notifications, et déterminer les données modifiées d'après ces notifications. Le module ACL assure la mise en forme des données modifiées et leur transfert sous la forme de messages au module de communication MSGF, en vue de permettre leur traitement successivement par les modules DCF, SYF, SAF et STF.

[0039] Durant une phase d'initialisation, le module CLD assure également le téléchargement d'une image de la base de données ADDB. Les données ainsi téléchargées sont également mises en forme et transférées par le module ACL au module de communication MSGF pour être traitées par les modules DCF, SAF et STF. Le traitement de mise en forme réalisé par le module ACL, appliqué aux données téléchargées et reçues dans les notifications, peut consister à sérialiser les données relatives aux objets de la base de données ADDB et les convertir dans un format textuel, par exemple JSON (JavaScript Object Notation), associant des étiquettes correspondant à des noms de types d'objets et d'attributs, et à des valeurs correspondant aux noms et valeurs des objets et des attributs.

[0040] Le module de décodage DCF assure le filtrage des données pour ne conserver que les données identifiées comme utiles à l'analyse de sécurité et la transcription en texte ou en caractères alphanumériques de certaines des éventuelles données binaires contenues dans les données utiles fournies par le module ACL. Ces traitements sont également appliqués aux données de la base de données ADDB recueillies durant la phase d'initialisation.

[0041] Le module de synchronisation SYF réordonne temporellement les messages issus du module de décodage DCF. En effet, il peut se produire que certains messages générés

par le module ACL ne soient pas produits ou reçus dans un ordre chronologique, de sorte qu'une modification opérée dans la base de données ADDB résultant d'une autre modification soit traitée par le module ACL avant cette autre modification. Le module SYF peut se baser sur un horodatage effectué par le module CSM qui attribue à cet effet une date et heure de réception à chaque notification reçue.

[0042] Le module d'analyse SAF analyse individuellement chaque modification de la base de données ADDB, issue du module de synchronisation SYF pour déterminer si la modification peut avoir une incidence sur la sécurité du réseau d'ordinateurs ou peut révéler une attaque. Si la modification est susceptible de compromettre la sécurité du réseau, le module SAF génère un message d'alerte contenant les données relatives à la modification et éventuellement un indice de criticité de la modification vis-à-vis de la sécurité du réseau. Le message d'alerte peut être transmis à une interface utilisateur ou être stocké dans un journal d'événements. Cette analyse est également appliquée aux données de la base de données ADDB recueillies durant la phase d'initialisation. Toutes les données ainsi traitées par le module SAF sont stockées dans la base de données locale DBI par le module STF. Ainsi la base de données locale DBI contient une image de la base de données ADDB recueillie durant la phase d'initialisation, et filtrée par le module DCF, ainsi que toutes les mises à jour des objets filtrés, opérées sur la base de données ADDB et notifiées au module CLD. Les données dans la base DBI sont en format alphanumérique ou en d'autres formats structurés bien identifiés (par exemple en format date), y compris les valeurs des objets et des attributs d'objet se trouvant dans la base de données.

[0043] Selon un mode de réalisation, l'analyse opérée par le module d'analyse SAF comprend au moins pour certains types de données modifiées, la recherche dans la base de données DBI d'une version précédente de la donnée modifiée, pour déterminer si la modification peut affecter la sécurité du réseau.

[0044] Selon un mode de réalisation, le module de communication MSGF gère une mémoire tampon d'entrée pour chacun des modules DCF, SYF, SAF et STF, dans laquelle il insère les données à traiter par le module. Chacun des modules DCF, SYF, SAF et STF extrait de sa mémoire tampon la donnée la plus ancienne pour la traiter. A chaque fois qu'une donnée est traitée par un module, la donnée traitée est insérée dans la mémoire tampon du module suivant devant traiter la donnée. A chaque fois que l'un des modules DCF, SYF, SAF et STF termine le traitement d'une donnée, il procède au traitement de la donnée la plus ancienne suivante dans sa mémoire tampon. Ainsi, les modules DCF, SYF, SAF et STF peuvent fonctionner d'une manière totalement désynchronisée, les uns par rapport aux autres. Cette disposition permet en outre d'exécuter simultanément plusieurs instances du même module lorsque la capacité de traitement du module est insuffisante par rapport à la cadence d'arrivée de nouvelles données à

traiter dans sa mémoire tampon. Ainsi, une nouvelle instance d'un des modules DCF, SYF, SAF et STF peut être activée dès qu'une donnée à traiter par ce module apparaît dans sa mémoire tampon, cette instance étant désactivée à la fin du traitement de la donnée.

[0045] Le terminal PC peut comprendre un module d'interface utilisateur UI configuré pour accéder aux messages d'alerte émis par le module d'analyse SAF, et générer des alarmes en fonction des indices de criticité associés aux messages. L'interface utilisateur UI peut également être configurée pour afficher ces alarmes ou les transmettre à d'autres entités par exemple via une messagerie électronique, ou via une interface (par exemple de type API – Application Programming Interface) avec un autre système par exemple du type SIEM (Security Information And Event Management). A noter que l'interface utilisateur UI peut se trouver sur un autre équipement (ou plusieurs) susceptible de recevoir et traiter les messages d'alerte émis par le module SAF.

[0046] Le service Microsoft™ Active Directory, stocke également des données dans des fichiers GPF rassemblant des objets définissant des stratégies de groupe. Les stratégies de groupe permettent de contrôler l'accès aux données d'un ordinateur, la politique de sécurité et d'audit, l'installation de logiciels, les scripts de connexion et de déconnexion, la redirection des dossiers, et des paramètres de navigation sur Internet. Chaque stratégie de groupe peut être associé à un domaine, site ou unité d'organisation. Ainsi, plusieurs objets ordinateurs ou utilisateurs peuvent être contrôlés par une unique stratégie de groupe. Les stratégies de groupe sont analysées et appliquées à chaque démarrage d'un ordinateur et pendant l'ouverture d'une session d'utilisateur. La base de données ADDB comprend des objets stratégie de groupe établissant des liens entre les fichiers GPF et les ordinateurs et les utilisateurs du domaine. Les fichiers GPF sont gérés par un système de fichiers distribués DFS, et sont rendus accessibles en dehors du serveur PDS par un module d'accès SMC implémentant le protocole SMB (Server Message Block).

[0047] Selon un mode de réalisation, l'application de surveillance MNEG comprend un module de communication client CSM pour communiquer avec le module SMC du serveur PDS, et un module FSW de réception et de prétraitement de notifications de modification des fichiers GPF, reçues et transmis par le module CSM. Le module CSM met en œuvre le protocole d'accès aux fichiers GPF stockés par le server PDS (par exemple le protocole SMB). Durant une phase d'initialisation, le module CSM commande le téléchargement des fichiers GPF stockés par le serveur PDS, et transmet au module SMC des commandes pour être notifié de toute modification apportée aux fichiers GPF sur le serveur PDS.

[0048] Le module FSW assure le téléchargement des fichiers GPF lors de la phase d'initialisation, et des fichiers GPF modifiés spécifiés dans les notifications reçues. Le

module FSW assure également la mise en forme des fichiers téléchargés et leur transfert au module de communication MSGF pour être traités successivement par les modules DCF, SYF, SAF et STF. Le traitement de mise en forme réalisé par le module FSW peut consister à sérialiser les données contenues dans les fichiers GPF, et les convertir dans le même format textuel que celui utilisé par le module ACL.

[0049] La figure 3 représente des étapes S1 à S13 d'une procédure de configuration et de recueil de notifications de modifications apparaissant dans le service d'annuaire, selon un mode de réalisation. Les étapes S1 à S13 sont exécutées successivement par les modules CLD et LDC. A l'étape S1, le module CLD du terminal PC réalise des opérations d'initialisation d'une connexion au serveur PDS. Cette étape permet notamment d'introduire un identifiant du serveur PDS. A l'étape S2, le module CLD définit des options de connexion définissant la manière dont la connexion va être établie et va se dérouler. A l'étape S3, le module CLD émet une commande de connexion à destination du serveur PDS désigné lors de l'initialisation de la connexion. Cette commande de connexion vise à déterminer un protocole de communication à utiliser pour la communication. Si la connexion est établie, à l'étape S4, le module SMC sur le serveur PDS fournit une réponse à la commande de connexion. A l'étape S5, le module CLD teste un indicateur d'établissement de la connexion avec le serveur PDS. Si la connexion n'est pas établie, la procédure prend fin ou est exécutée à nouveau à partir de l'étape S1. Dans le cas contraire, l'étape S6 est exécutée. A l'étape S6, le module CLD tente de s'authentifier auprès du serveur PDS en fournissant des données d'authentification, par exemple un identifiant de connexion UID et un mot de passe PW. Durant cette étape, le serveur PDS exécute une procédure d'authentification demandant au terminal PC de fournir des données d'authentification UID, PW. A l'issue de cette procédure, le serveur PDS fournit le résultat de l'authentification. A l'étape S8, la procédure prend fin si le résultat de l'authentification est négatif, ou se poursuit à l'étape S9 dans le cas contraire. A l'étape S9, le module CLD transmet au serveur PDS des commandes conformes au protocole LDAP pour recueillir une image de la base de données ADDB. A l'étape S10, le module LDC sur le serveur PDS transmet tous les objets stockés dans la base ADDB. A l'étape S10, le module CLD reçoit et traite les objets reçus, puis les transmet au module MSGF. A l'étape S11, le module CLD transmet au serveur PDS des commandes CMD conformes au protocole LDAP pour configurer le serveur PDS afin qu'il notifie au terminal PC toutes les modifications opérées dans la base de données ADDB. A l'étape S12, le serveur PDS transmet un message d'accusé de réception de ces commandes à destination du terminal PC. L'étape S13 suivante est exécutée à chaque fois qu'une modification est effectuée dans la base de données ADDB. A cette étape, le serveur PDS transmet au terminal PC un message de notification NTF contenant une donnée modifiée, cor-

respondant aux commandes CMD émises à l'étape S11.

[0050] Les commandes CMD émises à l'étape S11 définissent des options et filtres de recherche d'objets dans la base de données ADDB. Les filtres et options de recherche choisis configurent une recherche asynchrone dans laquelle toute modification appliquée à un objet quelconque dans la base de données ADDB, y compris une suppression d'objet, fait l'objet de la transmission d'une notification NTF (étape S12) par le serveur PDS au terminal PC. Les données contenues dans les messages de notification NTF (étapes S13) peuvent être au format LDIF (LDAP Data Interchange Format).

[0051] La figure 4 représente des étapes S21 à S29 d'une procédure de recueil et de prétraitement d'événements relatives à des modifications opérées dans les fichiers GPF, selon un mode de réalisation. Les étapes S21 à S29 sont exécutées successivement par le module CSM sur le terminal PC et SMC sur le serveur PDS. A l'étape S21, le module CSM se connecte au serveur PDS en lui transmettant une commande de négociation en vue de déterminer les protocoles de communication utilisables pour la communication. A l'étape S22, le module SMC sur le serveur PDS fournit une réponse à la commande de négociation. A l'étape S23, le module CSM transmet au module SMC une commande d'établissement d'une session de communication déclenchant une procédure d'authentification de l'utilisateur exécutant l'application de surveillance MNEG. A l'étape S24, le module SMC fournit une réponse à la commande d'établissement de session. Les étapes suivantes S25 à S29 sont exécutées seulement si l'authentification a réussi. A l'étape S25, le module CSM transmet une commande de téléchargement des fichiers GPF stockés par le serveur PDS. Ces fichiers sont reçus à l'étape S26, puis prétraités par le module FSW.

[0052] A l'étape S27, le module CSM transmet au module SMC une commande CMD spécifiant des fichiers GPF à surveiller, par exemple sous la forme d'un ou plusieurs chemins de dossiers de fichiers, et des événements de modification se produisant dans ces fichiers. Ces événements peuvent concerner une modification de la taille, de la date de création, de la date de la dernière écriture, du nom de fichier ou de dossier dans lequel se trouve le fichier, ou encore la suppression d'un des fichiers GPF. A l'étape S28, le module SMC répond à la commande CMD émise à l'étape S25 en émettant un message d'accusé réception. Les réponses émises par le module SMC aux étapes S22, S24, S26 et S28 peuvent signaler une erreur. Dans ce cas, le module CSM met fin à la procédure ou exécute à nouveau la commande précédente ou reprend la procédure depuis l'étape S21.

[0053] A chaque fois qu'une modification ayant l'un des types spécifiés, est effectuée dans l'un des fichiers GPF spécifiés dans la commande CMD transmise à l'étape S27, le module SMC transmet au module CSM un message de notification NTF contenant un

type de donnée modifié ou un type de modification, ainsi que le fichier GPF modifié ou les éléments modifiés dans ce fichier ou simplement le chemin d'accès à ce fichier (étape S29).

[0054] Les informations contenues dans chaque message de notification NTF sont traitées par le module FSW pour générer un message contenant les données modifiées, qui est transmis au module MSGF. Si le message de notification NTF reçu du serveur PDS indique simplement le nom ou le chemin d'accès vers le fichier GPF modifié, le module FSW accède au fichier sur le serveur PDS, par un processus de partage de fichiers, et met en forme les données du fichier en repérant les différents champs du fichier, en attribuant un nom textuel à chacun des champs ainsi repérés. Le fichier ainsi modifié est ensuite traité successivement par les modules DCF, SYF et SAF.

[0055] Le module de décodage DCF assure le filtrage des données utiles à l'analyse de sécurité et la transcription en texte ou caractères alphanumériques des éventuelles données binaires contenues dans les données utiles des fichiers fournis par le module FSW. Ces traitements sont également appliqués aux fichiers GPF recueillis durant la phase d'initialisation.

[0056] Comme précédemment pour les données de la base de données ADDB, le module SAF compare les données du fichier fourni par le module SYF, métadonnées comprises, avec la version précédente du fichier stockée dans la base de données DBI (le cas échéant celle acquise à l'étape S26) pour localiser, puis extraire les données modifiées de ce fichier, et applique à chaque donnée modifiée différents algorithmes de détection de faille de sécurité en fonction du type de la données modifiée. Si une faille de sécurité est ainsi détectée, le module SAF génère un message d'alerte contenant les données relatives à la modification et éventuellement un indice de criticité de la modification vis-à-vis de la sécurité du réseau. Comme précédemment, le message d'alerte peut être transmis à l'interface utilisateur UI ou être stocké dans un journal d'événements. Cette analyse est également appliquée aux fichiers GPF recueillis durant la phase d'initialisation. Toutes les données ainsi traitées par le module SAF sont ensuite stockées dans la base de données locale DBI par le module STF. Ainsi la base de données locale DBI contient une image des fichiers GPF, recueillie durant la phase d'initialisation, le contenu de ces fichiers étant filtré par le module DCF, ainsi que toutes les mises à jour des fichiers filtrés, appliquées aux fichiers GPF du serveur PDS et notifiées au module CSM lors des étapes S29.

[0057] De cette manière, la mise en place de fonctions de collecte de données de la base ADDB et de détection de faille de sécurité et d'attaque ne nécessite pas l'installation d'agents logiciels sur le serveur PDS. Par ailleurs, une fois qu'une copie de la base ADDB a été transmise au terminal PC durant une phase d'initialisation, seules les données modifiées sont transmises entre le serveur PDS et le terminal PC, ce qui

permet de limiter le flux de données transmises par le réseau à ce qui est nécessaire à la détection d'attaques. En outre, les fonctions de configuration des notifications de modifications des données du service d'annuaire permettent au terminal PC d'être informé en temps réel de toutes les modifications intervenues dans le service d'annuaire, contrairement à l'exploitation de journaux susceptibles d'être générés par le service d'annuaire. Il peut être observé également que ces fonctions de notification ne nécessitent pas de droits d'accès de niveau administrateur, seuls les droits d'accès d'un simple utilisateur étant requis pour permettre au terminal PC d'accéder, sur le serveur PDS, aux données de service d'annuaire pertinentes pour effectuer des analyses de sécurité.

[0058] Selon un mode de réalisation, le module SAF comprend une fonction d'analyse spécifique par type d'événement ou de donnée modifiée, et une fonction qui reçoit un type d'événement ou de donnée à traiter et qui appelle la fonction d'analyse correspondant au type d'événement ou de donnée reçu.

[0059] Selon un mode de réalisation, le module SAF peut être configuré pour analyser des paramètres de sécurité mémorisés dans la base de données ADDB ou dans les fichiers GPF et pour émettre un message d'alerte lorsqu'un de ces paramètres est fixé à une valeur introduisant une faille de sécurité. Ces paramètres de sécurité peuvent concerner les méthodes d'authentification employées pour authentifier les différents groupes d'utilisateurs du domaine du serveur PDS, les règles de choix des mots de passe, les droits d'accès attribués aux différents groupes d'utilisateurs, et les droits d'accès attribués à des fichiers répertoriés comme sensibles.

[0060] Pour traiter certains types de données, le module SAF peut être configuré pour comparer la valeur courante d'une donnée modifiée avec la valeur précédente de cette donnée stockée dans la base de données locale DBI, et générer un message d'alerte si cette comparaison peut révéler une faille de sécurité ou une attaque du réseau.

[0061] Pour traiter certains autres types de données afin de détecter une faille de sécurité ou une attaque du réseau, le module SAF peut être configuré pour comparer la valeur courante d'une donnée modifiée avec un certain nombre de valeurs précédentes de cette donnée, stockées dans la base de données locale DBI.

[0062] Pour traiter certains autres types de données afin de détecter une faille de sécurité ou une attaque du réseau, le module SAF peut être configuré pour rechercher une corrélation entre la valeur courante d'une donnée modifiée et la valeur d'une ou plusieurs autres données de la base de données locale DBI. Cette corrélation peut prendre en compte plusieurs valeurs précédentes des données considérées et/ou tenir compte d'un temps écoulé entre les dernières modifications des données considérées.

[0063] Lorsque le terminal PC reçoit une notification de donnée supprimée de la base ADDB ou de suppression d'un des fichiers GPF, la donnée supprimée ou les données

du fichier supprimé sont enregistrées dans la copie locale DBI à une valeur spécifique représentant l'état supprimé.

[0064] Le module SAF peut par exemple être configuré pour détecter dans un fichier GPF la présence de mots de passe en clair ou encodé de manière réversible. En effet, un fichier GPF peut contenir des données définies par les utilisateurs, et il est courant qu'un administrateur de réseau utilise cette possibilité pour mémoriser des données confidentielles telles que des mots de passe, la présence d'un tel mot de passe facilement accessible pouvant constituer une faille de sécurité pour le réseau. Le module SAF peut ainsi être configuré pour traiter un événement de création ou de modification d'un fichier GPF, en recherchant dans le fichier créé ou modifié la présence d'un mot de passe en clair ou encodés de manière réversible, par exemple en appliquant une méthode heuristique, et pour générer un message d'alerte s'il est probable que le fichier contient un mot de passe en clair.

[0065] Le module DAG peut enregistrer dans la base de données ADDB un nombre de tentatives erronées de connexion à un compte utilisateur. Le module SAF peut être configuré pour analyser ce type d'événement et lui attribuer un indice de criticité élevé si le nombre de tentatives erronées dépasse une certaine valeur de seuil. Le module SAF peut également corréler cet événement avec d'autres événements identiques concernant le même compte utilisateur en analysant les messages précédemment stockés dans l'unité de stockage DBI, pour évaluer l'indice de criticité à attribuer à l'événement.

[0066] Le module DAG peut enregistrer dans la base de données ADDB un changement de droit d'accès à un fichier ou de droit d'accès attribué à un utilisateur ou un ordinateur du réseau. Le module SAF peut être configuré pour analyser ce type d'événement et lui attribuer un indice de criticité élevé si ce changement de droit d'accès attribue par exemple à un utilisateur n'ayant aucun droit d'administrateur un accès à un fichier protégé dont l'accès est initialement restreint aux administrateurs du réseau, ou étend les droits d'accès de l'utilisateur ou de l'ordinateur.

[0067] Selon un mode de réalisation, le module DAG peut être configuré pour enregistrer dans la base de données ADDB les configurations logicielles de tous les ordinateurs et serveurs du domaine du serveur PDS. Le module SAF peut alors être configuré pour analyser les configurations logicielles des ordinateurs et serveurs du domaine enregistrées dans la base de données ADDB et pour émettre un message d'alerte lorsqu'un des ordinateurs exécute une version obsolète du système d'exploitation ou d'une application, ou lorsque le système d'exploitation ou une application ne dispose pas des derniers correctifs de sécurité.

[0068] Selon un mode de réalisation, le module SAF peut être configuré pour rechercher si des comptes utilisateurs dormants sont utilisés ou s'il existe des comptes utilisateurs

dormants ayant des droits d'accès élevés.

[0069] Il apparaîtra clairement à l'homme de l'art que la présente invention est susceptible de diverses variantes de réalisation et diverses applications. En particulier, la mise en place d'un service de notification de modifications intervenues dans les données d'un service d'annuaire n'est pas limitée à la détection d'attaques dirigées contre ce service d'annuaire, mais peut également être utilisée dans le cadre d'un archivage de ces modifications ou dans le but de procéder à des analyses statistiques appliquées à ces modifications, on encore de reconstruire une copie locale des données du service d'annuaire. Dans ce cas, le module de décodage DCF peut ne procéder à aucun filtrage des données de service d'annuaire reçues du serveur PDS.

[0070] Par ailleurs, d'autres méthodes peuvent être utilisées pour détecter des changements dans un service d'annuaire. Par exemple, une copie des données du service d'annuaire peut être acquise périodiquement, et une comparaison avec la copie précédente peut être réalisée afin de détecter toutes les modifications intervenues depuis la réalisation de la copie précédente. A l'issue de la comparaison, la copie précédente est remplacée par la dernière copie des données du service d'annuaire, ou bien seules les données modifiées sont ajoutées à la copie initiale. Chaque modification ainsi détectée peut ensuite être traitée individuellement comme si elle était issue d'une notification de modification des données du service d'annuaire.

Revendications

[Revendication 1] Procédé de collecte de données d'un service d'annuaire utilisé pour administrer un réseau privé comprenant un ensemble d'ordinateurs (SV1-SV3, DS1,DS2, P1-P7) interconnectés, le service d'annuaire rassemblant des données relatives à des objets du réseau, le procédé comprenant des étapes consistant à :
connecter un terminal (PC) à un serveur du réseau (PDS) comprenant une instance (ADDB, GPF) du service d'annuaire,
configurer l'instance du service d'annuaire sur le serveur par le terminal, pour que le terminal soit notifié de modifications apportées aux données du service d'annuaire,
recevoir par le terminal des messages de notification (NTF) contenant des données modifiées du service d'annuaire, transmis par le serveur, et traiter chacun des messages de notification reçu pour déterminer les modifications apportées aux données du service d'annuaire.

[Revendication 2] Procédé selon la revendication 1, comprenant des étapes consistant à :
télécharger, par le terminal (PC), les données du service d'annuaire (ADDB, GPF) dans une copie locale (DBI) gérée par le terminal, et
à chaque réception d'un message de notification (NTF) par le terminal, insérer dans la copie locale la valeur courante de la donnée modifiée indiquée dans le message de notification.

[Revendication 3] Procédé selon la revendication 1 ou 2, dans lequel des données du service d'annuaire sont stockées dans une base de données (ADDB) gérée par le serveur (PDS), un des messages de notification (NTF) contenant une nouvelle valeur d'une donnée du service d'annuaire, le procédé comprenant des étapes consistant à :
comparer la donnée modifiée à une valeur précédente de la donnée modifiée mémorisée dans une copie locale (DBI) gérée par le terminal, pour identifier un type de modification, et
insérer la nouvelle valeur de la donnée modifiée dans la copie locale.

[Revendication 4] Procédé selon l'une des revendications 1 à 3, dans lequel des données du service d'annuaire sont stockées dans des fichiers (GPF) gérés par le serveur (PDS), un des messages de notification contenant une référence à un fichier modifié et un type de modification apportée au fichier, le procédé comprenant des étapes consistant à :
télécharger par le terminal (PC) le fichier modifié indiqué dans le message de notification,

comparer le fichier téléchargé à une version précédente du fichier modifié mémorisée dans une copie locale (DBI) gérée par le terminal, pour identifier les données modifiées dans le fichier, et
insérer le fichier téléchargé ou les données modifiées du fichier dans la copie locale.

[Revendication 5] Procédé selon l'une des revendications 2 à 4, comprenant une étape de filtrage par le terminal (PC) des données du service d'annuaire reçues pour en extraire des données pertinentes pour détecter des anomalies, seules les données ainsi extraites étant stockées dans la copie locale (DBI).

[Revendication 6] Procédé selon l'une des revendications 2 à 5, comprenant une étape de conversion des données de service d'annuaire reçues par le terminal (PC) en format alphanumérique ou en données structurées avant de les stocker dans la copie locale (DBI).

[Revendication 7] Procédé de protection d'un réseau privé comprenant un ensemble d'ordinateurs interconnectés (SV1-SV3, DS1, DS2, P1-P7), le réseau étant administré par l'intermédiaire d'un service d'annuaire rassemblant des données de service d'annuaire relatives à des objets du réseau, le procédé comprenant des étapes consistant à :
mettre en œuvre par un terminal (PC) le procédé de collecte de données de service d'annuaire selon l'une des revendications 1 à 6, pour acquérir des données d'une instance de service d'annuaire d'un serveur (PDS) du réseau, gérant le service d'annuaire,
stocker les données de service d'annuaire acquises dans une copie locale (DBI) gérée par le terminal,
à chaque fois qu'un message de notification (NTF) de modification d'une donnée du service d'annuaire est reçue, analyser par le terminal, la donnée modifiée par rapport aux données de service d'annuaire stockées dans la copie locale, pour déterminer si une modification appliquée aux données du service d'annuaire génère une faille de sécurité du réseau ou révèle une attaque du réseau, et
générer un message d'alerte en cas de détection d'une faille de sécurité ou d'une attaque du réseau.

[Revendication 8] Procédé selon la revendication 7, dans lequel l'analyse de la donnée modifiée comprend des étapes consistant à :
rechercher dans la copie locale (DBI) une valeur précédente de la donnée modifiée, et
comparer la valeur courante de la donnée modifiée à la valeur

précédente de la donnée modifiée, un message d'alerte étant généré si la comparaison révèle l'apparition d'une faille de sécurité ou une attaque du réseau.

[Revendication 9] Procédé selon la revendication 8, dans lequel l'analyse d'une donnée modifiée comprend des étapes consistant à :
rechercher dans la copie locale (DBI) plusieurs valeurs précédentes de la donnée modifiée, et
comparer entre elles la valeur courante de la donnée modifiée et les valeurs précédentes de la donnée modifiée, un message d'alerte étant généré si la comparaison révèle l'apparition d'une faille de sécurité ou une attaque du réseau.

[Revendication 10] Procédé selon la revendication 9, dans lequel l'analyse d'une donnée modifiée comprend des étapes consistant à :
rechercher dans la copie locale (DBI) la valeur d'au moins une donnée corrélée à la donnée modifiée, et
déterminer si la valeur courante de la donnée modifiée considérée en corrélation avec la valeur de la donnée corrélée, révèle l'apparition d'une faille de sécurité ou une attaque du réseau.

[Revendication 11] Procédé selon l'une des revendications 1 à 10, dans lequel les objets du réseau comprennent des serveurs (SV1-SV3, DS1-DS2, PDS), des terminaux d'utilisateurs (P1-P7, PC), des appareils périphériques (I1-I3), des utilisateurs, des groupes d'utilisateurs, des services,

[Revendication 12] Terminal configuré pour mettre en œuvre le procédé selon l'une des revendications 1 à 11.

[Revendication 13] Produit programme d'ordinateur directement chargeable dans une mémoire interne d'un ordinateur et comprenant des portions de code qui lorsqu'elles sont exécutées par un ordinateur configurent l'ordinateur pour mettre en œuvre le procédé selon l'une des revendications 1 à 11.

[Fig. 1]

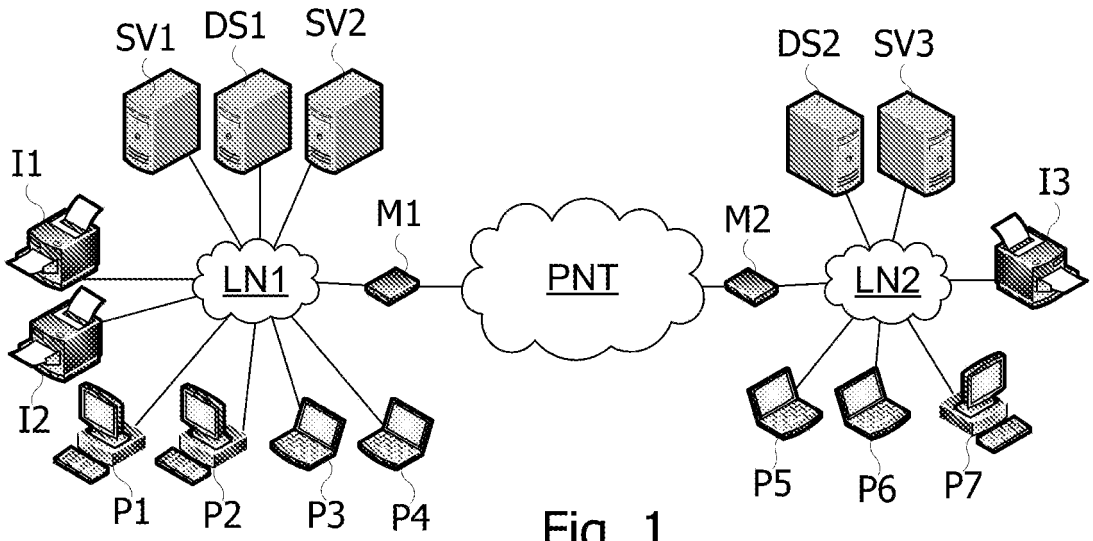
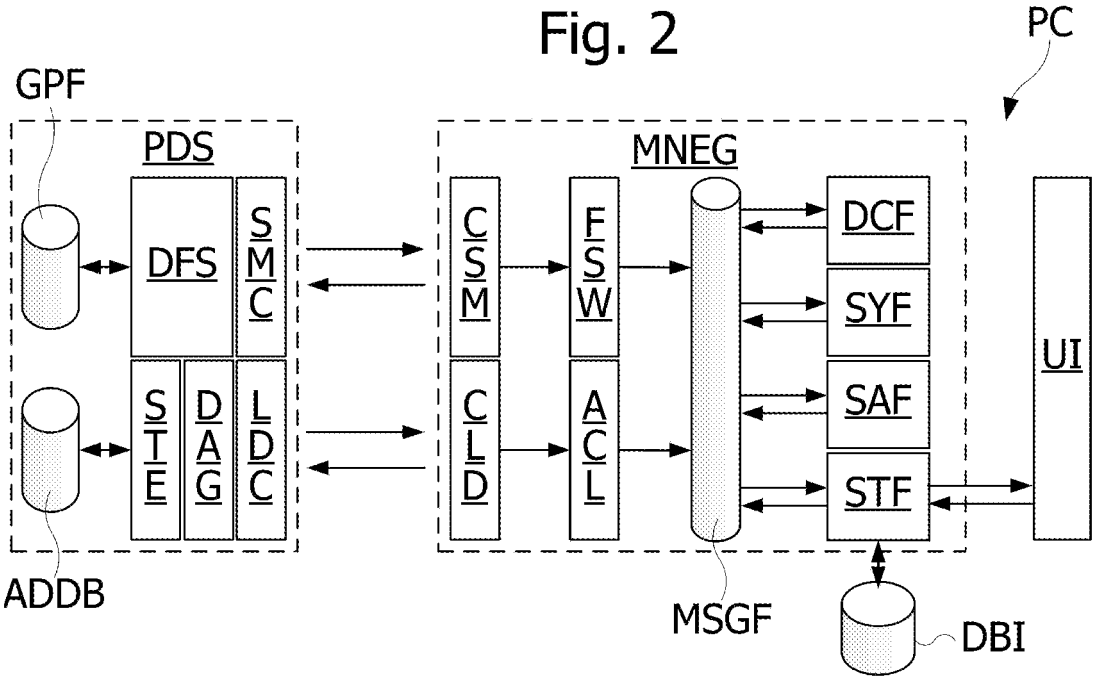


Fig. 1

[Fig. 2]

Fig. 2



[Fig. 3]

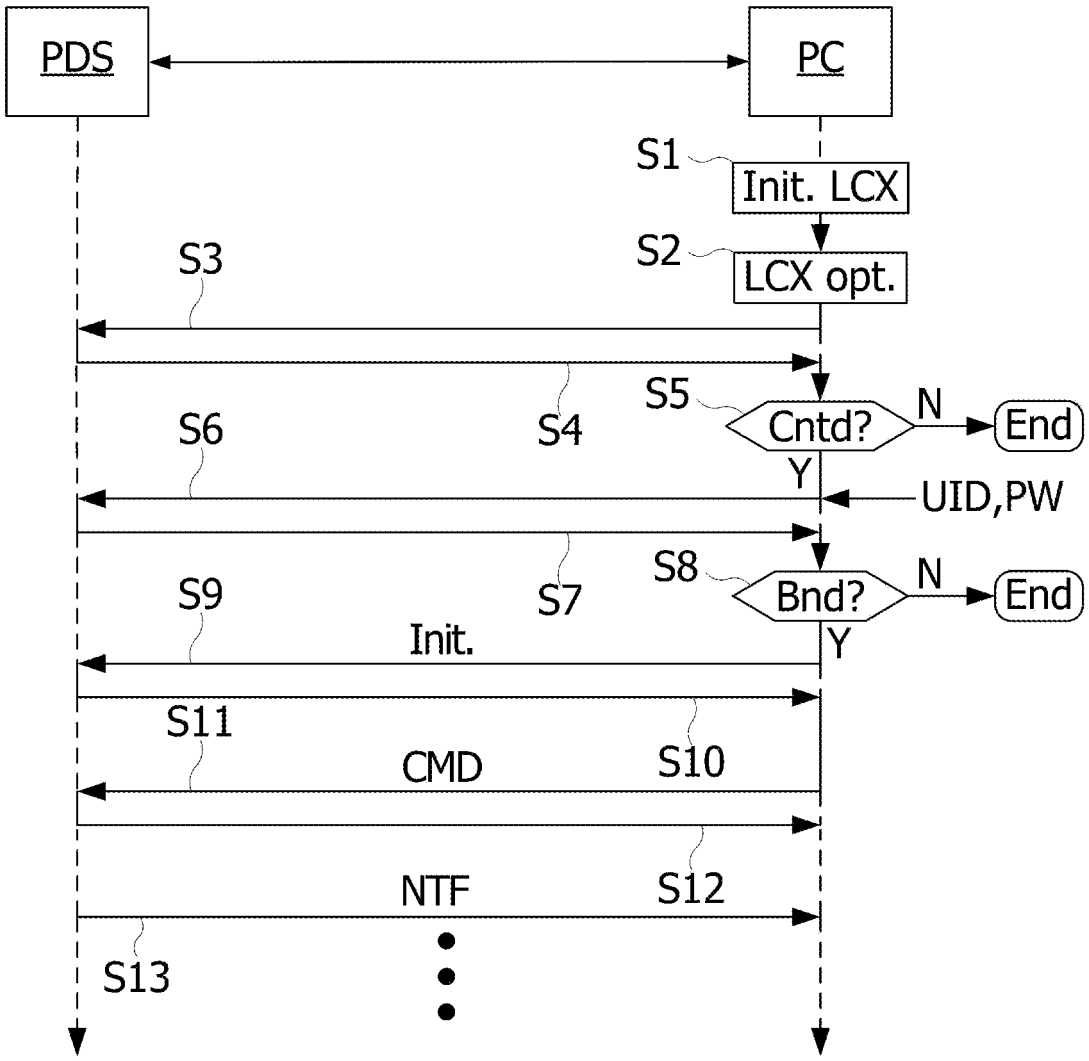

PDS
PC
S1
Init. LCX
S2
LCX opt.
S3
S4
S5
Cntd?
N
End
Y
S6
UID,PW
S7
S8
Bnd?
N
End
Y
S9
Init.
S10
S11
CMD
S12
NTF
S13

Fig. 3

[Fig. 4]

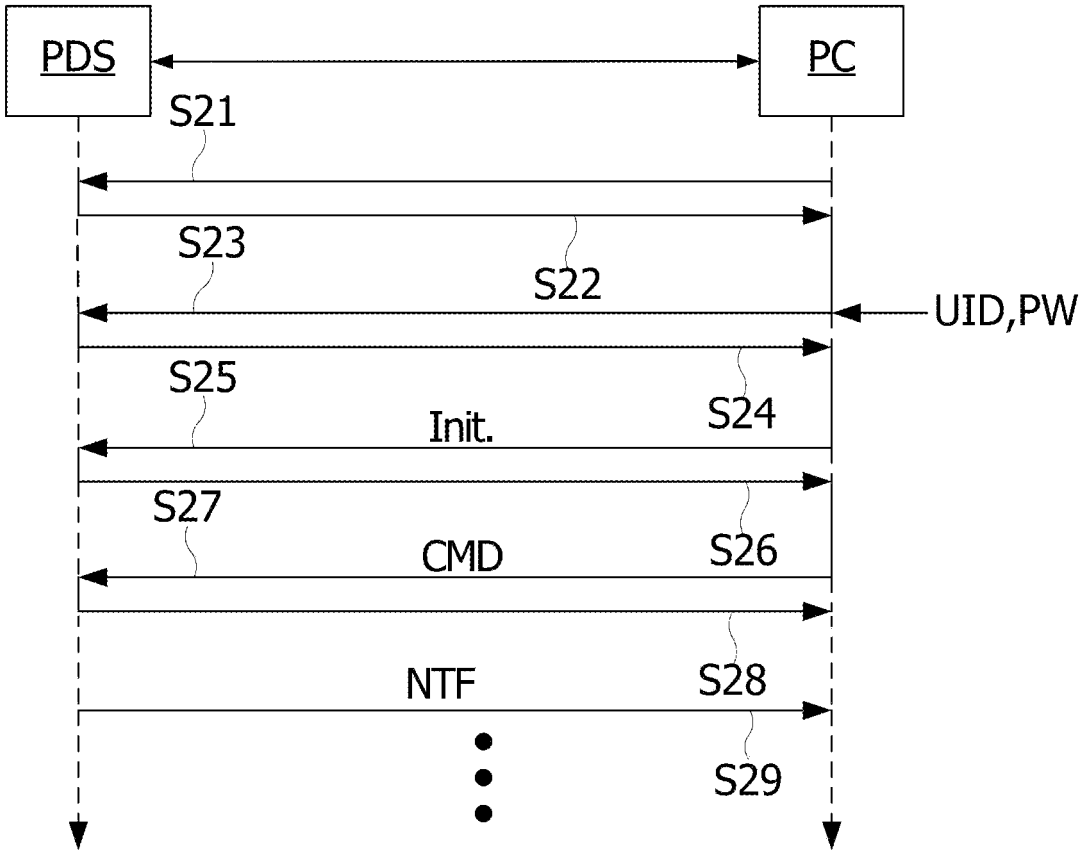


Fig. 4

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 865412
FR 1901975

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	US 5 862 325 A (REED DRUMMOND SHATTUCK [US] ET AL) 19 janvier 1999 (1999-01-19) * colonne 1, ligne 1 - colonne 94, ligne 67 *	1-13	H04L12/26 G06F21/57
X	US 2015/234910 A1 (SCHIFF OLIVER [DE] ET AL) 20 août 2015 (2015-08-20) * alinéa [0001] - alinéa [0063] *	1-13	

DOMAINES TECHNIQUES RECHERCHÉS (IPC)

H04L

Date d'achèvement de la recherche	Examinateur
14 octobre 2019	García Bolós, Ruth

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons
.....
& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 1901975 FA 865412

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 14-10-2019
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 5862325 A	19-01-1999	AU 702509 B2	25-02-1999
		EP 0954782 A1	10-11-1999
		US 5862325 A	19-01-1999
		US 6088717 A	11-07-2000
		WO 9732251 A1	04-09-1997
US 2015234910 A1	20-08-2015	AU 2015218203 A1	29-09-2016
		EP 3108417 A1	28-12-2016
		US 2015234910 A1	20-08-2015
		WO 2015123680 A1	20-08-2015

EPO FORM P0465