(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 962 283**

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

(21) **N° d'enregistrement national :** **10 02772**

(51) Int Cl[8] : ***H 04 L 29/06*** *(2006.01), H 04 L 9/00*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 30.06.10.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 06.01.12 Bulletin 12/01.

(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 :**

(71) **Demandeur(s) :** *ALCATEL LUCENT Société anonyme* — FR.

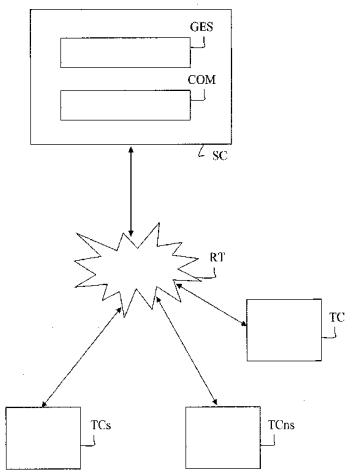
(72) **Inventeur(s) :** BERTRAND DANIEL et BORSCHNECK PASCAL.

(73) **Titulaire(s) :** ALCATEL LUCENT Société anonyme.

(74) **Mandataire(s) :** ALCATEL LUCENT INTERNATIONAL.

(54) CONTROLE DE COMMUNICATION SECURISEE.

(57) Pour contrôler une communication entre au moins un terminal sécurisé (TCs) et un terminal non sécurisé (TCns) par l'intermédiaire au moins du serveur (SC) à travers un réseau de télécommunications (RT), le terminal sécurisé étant apte à transmettre et recevoir des flux de média chiffrés et le terminal non sécurisé n'étant pas apte à transmettre et recevoir des flux de média chiffrés, le serveur (SC) transmet un message (MesS) au terminal sécurisé (TCs), le message (MesS) contenant une information indiquant que la communication entre le terminal sécurisé (TCs) et le terminal non sécurisé (TCns) n'est pas sécurisée, suite à une réception d'un message (MesT) transmis depuis le terminal non sécurisé (TCns), le message (MesT) contenant un paramètre de sécurité indiquant qu'au moins un flux de média transmis depuis le terminal non sécurisé (TCns) n'est pas chiffré.



FR 2 962 283 - A1

CONTROLE DE COMMUNICATION SECURISEE

La présente invention concerne un contrôle d'une communication entre au moins deux terminaux dans un réseau de télécommunications pour vérifier si la communication est sécurisée par rapport à chacun des terminaux.

Actuellement, un terminal de type SIP ("Session Initiation Protocol" en anglais) peut déterminer si une communication multimédia en cours établie avec une autre entité directement liée au terminal est sécurisée entre le terminal et l'autre entité, et peut en informer l'utilisateur du terminal par exemple au moyen d'un signal lumineux. La communication multimédia peut consister à un échange de données telles que des flux vidéo, audio ou de messages instantanés dont l'établissement est réalisé via le protocole SIP.

Le flux de média reçu par le terminal peut résulter d'un ou plusieurs flux de média dont au moins un n'est pas sécurisé. Par exemple, le flux de média reçu par le terminal résulte d'une conversion par un serveur d'un autre flux de média non sécurisé, ou de l'addition d'au moins un autre flux de média non sécurisé à une conférence gérée par un serveur.

Dans ce cas, bien que le flux de média reçu par le terminal soit sécurisé entre le terminal et un serveur qui est directement lié au terminal et duquel provient le flux de média, le terminal peut indiquer à l'utilisateur un état sécurisé de la communication qui est erroné puisque l'ensemble de la communication n'est pas sécurisé. Ainsi, l'utilisateur croira à tort que la communication en cours est sécurisée alors qu'au moins une partie de la communication n'est pas sécurisée, ce qui rend l'ensemble de la communication non sécurisée.

Un objectif de l'invention est de remédier aux inconvénients précédents en vérifiant si une communication établie entre au moins deux terminaux via au moins un serveur dans un réseau de télécommunications est sécurisée de bout en bout.

Pour atteindre cet objectif, un procédé selon l'invention pour contrôler une communication entre au moins un terminal sécurisé et un terminal non sécurisé par l'intermédiaire d'au moins un serveur à travers un réseau de télécommunications, le terminal sécurisé étant apte à transmettre et recevoir des flux de média chiffrés et

le terminal non sécurisé n'étant pas apte à transmettre et recevoir des flux de média chiffrés, comprenant dans le serveur :

suite à une réception d'un message transmis depuis le terminal non sécurisé, le message contenant une information indiquant que la communication entre le terminal non sécurisé et le serveur n'est pas sécurisée,

une transmission d'un message au terminal sécurisé, le message contenant un paramètre de sécurité indiquant que la communication entre le terminal sécurisé et le terminal non sécurisé n'est pas sécurisée.

Avantageusement, l'utilisateur du terminal sécurisé est informé de l'état sécurisé ou non sécurisé de l'ensemble de la communication à laquelle il participe, et pas seulement d'une partie de la communication correspondant à des échanges entre le terminal sécurisé et le serveur.

Ainsi, lorsqu'un terminal non sécurisé se joint à une communication à laquelle participe un terminal sécurisé, l'utilisateur du terminal sécurisé est informé que la communication n'est plus sécurisée, c'est-à-dire qu'au moins un flux de média reçu par le serveur depuis un terminal non sécurisé n'est pas chiffré.

Selon d'autres caractéristiques de l'invention, le paramètre de chiffrement contenu dans le message transmis au terminal sécurisé peut être associé à un type de média, indiquant que le flux de média correspondant au type de média n'est pas chiffré, peut être en outre associé à un type de chiffrement qui définit des caractéristiques d'un algorithme de chiffrement à utiliser pour chiffrer et déchiffrer un flux de média, et peut être en outre associé à une indication sur le terminal non sécurisé pour lequel la communication avec le serveur n'est pas sécurisée.

Selon d'autres caractéristiques de l'invention, les flux de média échangés lors de la communication peuvent être conformes au protocole SIP, et le message transmis au terminal sécurisé peut être l'un des messages de type "INVITE", "RE-INVITE", "200 OK", et "UPDATE" conformes au protocole SIP.

Selon une autre caractéristique de l'invention, le paramètre de chiffrement contenu dans le message transmis au terminal sécurisé peut être inclus dans un en-tête dans ledit message.

Selon une autre caractéristique de l'invention, le paramètre de chiffrement contenu dans le message transmis au terminal sécurisé peut être inclus dans un

sous-message qui est encapsulé dans ledit message et qui comporte des données utilisables par la couche transport.

L'invention concerne encore un serveur pour contrôler une communication entre au moins un terminal sécurisé et un terminal non sécurisé par l'intermédiaire au moins du serveur à travers un réseau de télécommunications, le terminal sécurisé étant apte à transmettre et recevoir des flux de média chiffrés et le terminal non sécurisé n'étant pas apte à transmettre et recevoir des flux de média chiffrés, comprenant :

des moyens pour transmettre un message au terminal sécurisé, le message contenant un paramètre de sécurité indiquant que la communication entre le terminal sécurisé et le terminal non sécurisé n'est pas sécurisée, suite à une réception d'un message transmis depuis le terminal non sécurisé, le message contenant une information indiquant que la communication entre le terminal non sécurisé et le serveur n'est pas sécurisée.

Selon d'autres caractéristiques de l'invention, le serveur peut héberger une conférence multimédia entre au moins le terminal sécurisé, le terminal non sécurisé et un autre terminal, ou bien le serveur peut être un serveur de média convertissant le format de flux de média échangés entre le terminal sécurisé et le terminal non sécurisé.

L'invention se rapporte encore à un programme d'ordinateur apte à être mis en œuvre dans un serveur, ledit programme comprenant des instructions qui, lorsque le programme est exécuté dans ledit serveur, réalisent les étapes selon le procédé de l'invention.

La présente invention et les avantages qu'elle procure seront mieux compris au vu de la description ci-après faite en référence aux figures annexées, dans lesquelles :

- la figure 1 est un bloc-diagramme schématique d'un système de communication pour vérifier si une communication établie entre au moins deux terminaux dans un réseau de télécommunications est sécurisée selon une réalisation de l'invention,

- la figure 2 est un algorithme d'un procédé pour vérifier si une communication établie entre au moins deux terminaux dans un réseau de télécommunications est sécurisée selon une réalisation de l'invention.

En référence à la figure 1, un système de communication selon l'invention comprend un réseau de télécommunications RT, au moins deux terminaux de communication TC aptes à communiquer entre eux via au moins un serveur de communication SC.

Le réseau de télécommunications RT peut être un réseau filaire ou sans fil, ou une combinaison de réseaux filaires et de réseaux sans fil.

Selon un exemple, le réseau de télécommunications RT est un réseau de paquets à haut débit de type IP ("Internet Protocol" en anglais), tel que l'internet ou un intranet.

De manière générale, on entend par "communication" une communication bipartite, c'est-à-dire un dialogue entre deux terminaux de communication, ou une conférence à laquelle participe aux moins trois terminaux de communication, un terminal de communication pouvant joindre une communication déjà existante entre n terminaux de communication participants avec $n \geq 2$. La communication est établie entre au moins deux terminaux via au moins un serveur de communication SC.

La communication est une communication multimédia au cours de laquelle sont échangées des données telles que des flux vidéo, audio ou de messages instantanés au moyen du protocole SIP. La communication entre un terminal et un serveur peut être bidirectionnelle ou unidirectionnelle, par exemple lorsque l'utilisateur du terminal est seulement en écoute.

On entend également par "communication sécurisée" une communication qui est chiffrée de bout en bout. Par exemple, lors d'une communication entre un terminal et un serveur, le terminal est apte à chiffrer des flux multimédias à transmettre vers le serveur qui est apte à déchiffrer les flux multimédias reçus, et inversement. Par ailleurs, seulement une partie des flux multimédias peut être chiffrée, tel que le flux vidéo, et une autre partie des flux multimédias peut ne pas être chiffrée, tel que le flux audio, dans ce cas la communication n'est pas considérée comme sécurisée.

A titre d'exemples, un terminal de communication TC est un téléphone fixe ou mobile, un dispositif ou objet électronique de télécommunications qui est personnel à l'utilisateur et qui peut être un assistant numérique personnel communicant PDA ("Personnal Digital Assistant" en anglais), ou un téléphone intelligent (SmartPhone), pouvant être relié à une borne d'accès d'un réseau public sans fil de faible portée du type WLAN ("Wireless Local Area Network" en anlais) ou conforme à l'une des normes 802.1x, ou de moyenne portée selon le protocole WIMAX ("World wide Interoperability Microwave Access" en anglais).

Le serveur de communication SC délivre des flux multimédias à au moins un terminal et/ou reçoit des flux multimédias depuis au moins un terminal. A titre d'exemples, un serveur de communication peut servir de pont pour une conférence multimédia entre plusieurs terminaux, ou peut servir de serveur de média convertissant le format de flux multimédias échangés entre au moins deux terminaux.

Par ailleurs, plusieurs serveurs de communications SC peuvent être impliqués dans une communication entre plusieurs terminaux. Dans un exemple, deux serveurs de communication peuvent communiquer entre eux et servir chacun de pont pour une conférence multimédia entre plusieurs terminaux. Dans un autre exemple, un serveur de communication peut servir de pont pour une conférence multimédia entre plusieurs terminaux, et un autre serveur de communication servant d'intermédiaire entre le pont de conférence et l'un des terminaux peut convertir un flux audio en un flux textuel à destination du terminal, ou bien modifier un taux de compression du flux audio à destination du terminal.

Par souci de clarté sont représentés sur la figure 1 un terminal de communication TCs dit "sécurisé", un terminal de communication TCns dit "non sécurisé", et un terminal de communication TC désignant indifféremment un terminal sécurisé TCs ou un terminal non sécurisé TCns, aptes à être en communication par l'intermédiaire d'un serveur de communication SC. Le terminal de communication sécurisé TCs implémente une fonction de chiffrement de flux multimédias à transmettre et de déchiffrement de flux multimédias reçus et est donc apte à transmettre et recevoir des flux multimédias sécurisés, tandis que le terminal de communication non sécurisé TCns n'implémente pas de fonction de chiffrement de flux multimédias et n'est pas apte à transmettre et recevoir des flux multimédias sécurisés.

Dans une variante, il est considéré qu'un terminal de communication non sécurisé TCns peut être assimilé à un serveur qui n'implémente pas l'invention. Selon un exemple, le terminal de communication non sécurisé TCns est assimilé à un serveur non sécurisé parmi plusieurs serveurs de communication communiquant entre eux et servant chacun de pont pour une conférence multimédia entre plusieurs terminaux. Selon un autre exemple, le terminal de communication non sécurisé TCns est assimilé à un serveur non sécurisé servant d'intermédiaire entre un pont de conférence multimédia entre plusieurs terminaux et l'un des terminaux participant à la conférence par exemple pour convertir des flux multimédias. Ainsi, il est considéré qu'un terminal de communication non sécurisé TCns, ici assimilé à un serveur non sécurisé, peut implémenter une fonction de chiffrement de flux multimédias et être apte à transmettre et recevoir des flux multimédias sécurisés, mais ne peut pas garantir que toutes les communications avec le terminal sont sécurisées. En d'autres termes, le terminal de communication non sécurisé TCns peut chiffrer un flux multimédia mais ne peut pas garantir que d'autres flux reçus utilisés pour produire le flux multimédia sont sécurisés.

Le serveur de communication SC comprend un module de communication COM et un module de gestion GES.

Dans la suite de la description, le terme module peut désigner un dispositif, un logiciel ou une combinaison de matériel informatique et de logiciel, configuré pour exécuter au moins une tâche particulière.

Le module de communication COM a pour fonctionnalité d'établir une communication avec des entités du réseau de télécommunication, par exemple avec un autre serveur ou un terminal et de transmettre des messages à ces entités.

Le module de gestion GES a pour fonctionnalité de déterminer l'état chiffré des flux multimédias relatifs à chacune des communications établies avec des terminaux ou des serveurs.

Comme indiqué précédemment, dans un mode de réalisation non limitatif, la communication est une communication multimédia établie au moyen du protocole de communication SIP (protocole d'établissement de session) qui est utilisé au niveau de la couche session pour l'établissement des communications multimédias tandis que le protocole de communication RTP ("Real-time Transport Protocol" en

anglais) et RTCP ("Real-time Transport Control Protocol" en anglais) est utilisé au niveau de la couche transport pour le transport des flux multimédias eux-mêmes.

On notera que le protocole SIP est destiné à des applications non limitatives telles que la voix sur IP, la visiophonie (voix sur IP plus vidéo sur IP), ou encore la messagerie instantanée (« chat » en anglais).

Le protocole SIP est défini par le groupe de standardisation IETF ("Internet Engineering Task Force" en anglais) en particulier dans les documents RFC3261 et RFC3265.

On notera qu'outre l'établissement d'appels multimédias, le protocole SIP se charge de l'authentification et de la localisation d'agents clients et se base sur un échange de requêtes (appelées également messages). Le protocole SIP ne transporte pas les données échangées durant la session comme la voix ou la vidéo. Comme il est indépendant de la transmission des données, tout type de protocole peut être utilisé pour cet échange, tel que le protocole RTP/RTCP. Cependant le protocole SIP encapsule dans ses propres requêtes des messages SDP ("Session Description Protocol" en anglais) comportant des données utilisables par la couche transport.

En référence à la figure 2, un procédé de contrôle de communication selon une réalisation de l'invention comprend des étapes E1 et E2 exécutées automatiquement dans le système de communication.

Le procédé est décrit ci-après conformément au protocole SIP en tant qu'exemple.

Il est considéré qu'un terminal de communication non sécurisé TCns se joint à une communication en cours d'établissement ou déjà établie, à laquelle participe au moins un autre terminal de communication sécurisé TCs par l'intermédiaire d'au moins un serveur de communication SC.

Selon un exemple, la communication est une conférence qui est hébergée par un serveur de communication SC et à laquelle participe déjà au moins deux terminaux de communication sécurisés TCs.

Selon un autre exemple, la communication est en cours d'établissement entre le terminal non sécurisé et un terminal sécurisé par l'intermédiaire d'un serveur de communication SC, la communication pouvant être à l'initiative du terminal non sécurisé ou du terminal sécurisé.

A l'étape E1, le terminal de communication non sécurisé TCns transmet un message MesT au serveur de communication SC pour établir une communication avec le terminal de communication sécurisé TCs.

Le message MesT contient une information indiquant que la communication entre le terminal non sécurisé TCns et le serveur SC n'est pas sécurisée.

Selon une réalisation, le message MesT comprend un champ renseigné par un paramètre de chiffrement Pc qui est à un état "0" si le terminal transmettant le message implémente une fonction de chiffrement de flux multimédias, et qui est à un état "1" si le terminal transmettant le message n'implémente pas une fonction de chiffrement de flux multimédias. En variante, le message MesT comprend un champ renseigné par un paramètre de chiffrement Pc qui a une valeur particulière, telle que "faux" si le terminal transmettant le message implémente une fonction de chiffrement de flux multimédias, et "vrai" si le terminal transmettant le message n'implémente pas une fonction de chiffrement de flux multimédias.

Le champ est par exemple un champ "a" de la forme suivante, lorsque le terminal transmettant le message est un terminal non sécurisé TCns :

a = secured-communication:false

Dans ce cas, le message MesT contient un paramètre de chiffrement Pc qui est une information indiquant que la communication entre le terminal non sécurisé TCns et le serveur SC n'est pas sécurisée.

Selon une autre réalisation, le message MesT ne comprend pas de champ renseigné par un paramètre de chiffrement Pc ni aucun paramètre indiquant que le terminal non sécurisé implémente une fonction de chiffrement de flux multimédias. Dans ce cas, le message MesT contient implicitement une information indiquant que la communication entre le terminal non sécurisé TCns et le serveur SC n'est pas sécurisée, cette information étant déduite de l'absence d'indication sur l'implémentation d'une fonction de chiffrement de flux multimédias par le terminal non sécurisé.

Selon encore une autre réalisation, le terminal de communication non sécurisé TCns est assimilé à un serveur non sécurisé, qui n'implémente pas l'invention. Le terminal de communication non sécurisé TCns peut implémenter une fonction de chiffrement de flux multimédias, étant apte à transmettre et recevoir des

flux multimédias sécurisés, mais ne peut pas garantir que toutes les communications avec le terminal non sécurisé TCns sont sécurisées.

Dans ce cas, le message MesT peut contenir un champ indiquant que la communication entre le terminal non sécurisé TCns et le serveur SC est chiffrée, par exemple au moyen d'un paramètre de chiffrement Pc, mais ne contient pas un paramètre, tel que le paramètre de sécurité Ps défini ci-après à l'étape E2, garantissant que la communication entre le terminal non sécurisé TCns et le serveur SC est sécurisée. Ainsi, le message MesT contient implicitement une information indiquant que la communication entre le terminal non sécurisé TCns et le serveur SC n'est pas sécurisée, cette information étant déduite de l'absence du paramètre de sécurité Ps.

Dans le cas présent, le terminal de communication non sécurisé TCns transmet un message MesT comprenant un paramètre de chiffrement Pc, qui est à un état "0" ou qui a une valeur "faux", indiquant que la communication entre le terminal de communication non sécurisé TCns et le serveur de communication SC n'est pas sécurisé, c'est-à-dire n'est pas chiffrée.

Optionnellement, le paramètre Pc est associé à un type de média, par exemple un média audio, vidéo ou textuel, indiquant quel flux de média n'est pas sécurisé.

Optionnellement, le paramètre Pc est associé à un type de chiffrement qui définit des caractéristiques d'un algorithme de chiffrement à utiliser pour chiffrer et déchiffrer un flux de média.

A titre d'exemple, le paramètre Pc, optionnellement le type de média et le type de chiffrement associés au paramètre Pc constituent un sous-message qui est encapsulé dans le message MesT, par exemple un message SDP encapsulé dans le message SIP.

A l'étape E2, le module de gestion GES du serveur de communication SC analyse le message MesT reçu et notamment le paramètre de chiffrement Pc.

Le module de gestion GES génère un message MesS comprenant un champ renseigné par un paramètre de sécurité Ps qui est à un état "0" si au moins un terminal ayant transmis le message MesT est un terminal non sécurisé TCns, et

qui est à un état "1" si tous les terminaux ayant transmis un message MesT sont des terminaux sécurisés TCs.

De manière générale, le paramètre de sécurité Ps contenu dans le message MesT destiné à être transmis vers un terminal de communication indique qu'au moins une communication entre le serveur de communication et une autre entité du réseau de télécommunication, telle qu'un autre serveur de communication ou un terminal de communication non sécurisé, n'est pas sécurisée, c'est-à-dire n'est pas chiffrée ou dont la sécurisation n'est pas garantie.

L'information indiquant que la communication n'est pas sécurisée est ainsi relayée à toutes les entités participant à la communication.

Selon un premier exemple, la communication est en cours d'établissement entre le terminal non sécurisé TCns et un terminal sécurisé TCs par l'intermédiaire du serveur de communication SC. Le module de communication COM du serveur SC transmet le message MesS comprenant le paramètre de sécurité Ps au terminal sécurisé TCs.

Si la communication est à l'initiative du terminal non sécurisé TCns, le message MesS est par exemple de type INVITE avec le paramètre Ps constituant un sous-message SDP encapsulé dans le message INVITE.

Si la communication est à l'initiative du terminal sécurisé TCs, le message MesS est par exemple de type 200 OK avec le paramètre Ps constituant un sous-message SDP encapsulé dans le message 200 OK. Initialement, les messages transmis depuis le terminal sécurisé TCs au serveur SC et du serveur SC au terminal non sécurisé TCns sont de type INVITE pour requérir l'établissement de la communication.

Selon un deuxième exemple, la communication est une conférence qui est hébergée par le serveur de communication SC et à laquelle participe déjà deux terminaux de communication sécurisés TCs. Le serveur de communication SC transmet le message MesS comprenant le paramètre de chiffrement Ps aux deux terminaux de communication sécurisés TCs. Le message MesS est par exemple de type RE-INVITE avec le paramètre Ps constituant un sous-message SDP encapsulé dans le message RE-INVITE, ou bien le message MesS est par exemple de type UPDATE avec le paramètre Ps constituant un en-tête du message UPDATE.

Comme indiqué précédemment, le paramètre Ps peut optionnellement être également associé à un type de média, par exemple un média audio, vidéo ou textuel, indiquant quel flux de média n'est pas sécurisé, et optionnellement associé à un type de chiffrement qui définit des caractéristiques d'un algorithme de chiffrement à utiliser pour chiffrer et déchiffrer un flux de média.

Le champ est par exemple un champ "a" de la forme suivante, lorsqu'un flux de média reçu par le serveur de communication lors d'une communication avec un terminal non sécurisé comprend un flux audio sécurisé et un flux vidéo non sécurisé :

a = secured-communication:audio=true;video=false

Optionnellement, le paramètre Ps est en outre associé à une indication sur le terminal non sécurisé pour lequel la communication avec le serveur de communication n'est pas sécurisée. Ainsi, lorsque trois terminaux sécurisés sont en conférence via le serveur de communication et qu'un terminal non sécurisé se joint à la conférence, le serveur de communication indique aux terminaux sécurisés que la conférence n'est plus sécurisée, notamment que la communication entre le serveur et le terminal ayant rejoint la conférence n'est pas sécurisée.

Selon une réalisation, le champ contenant le paramètre Ps dans le message MesS est un champ généré et ajouté au contenu du message MesS. Le paramètre Ps peut en outre être déduit du paramètre Pc si ce dernier est présent dans le message MesT reçu par le serveur de communication SC.

En variante, le message MesS contient déjà un champ contenant un paramètre pour indiquer si la communication est sécurisée entre le serveur de communication SC et le terminal de communication sécurisé TCns auquel est destiné le message MesS. Par exemple, lors d'une conférence entre plusieurs terminaux sécurisés, des messages transmis par le serveur de communication à chaque terminal sécurisé contiennent un paramètre indiquant que la communication est sécurisée entre le serveur de communication SC et le terminal de communication sécurisé, et lorsqu'un terminal non sécurisé se joint à la conférence, le serveur de communication transmet à chaque terminal sécurisé un message contenant le paramètre ayant une valeur modifiée et indiquant que la conférence n'est plus sécurisée.

Ainsi, les étapes du procédé ont été décrites dans un mode de réalisation non limitatif en utilisant le protocole SIP, mais bien entendu, d'autres protocoles peuvent être utilisés tel que dans un exemple non limitatif le protocole réseau numérique à intégration de services RNIS, (ISDN "Integrated Services Digital Network" en anglais). Dans ce cas, dans un exemple non limitatif, le message INVITE décrit précédemment peut être remplacé par un message SETUP, le message UPDATE peut être remplacé par un message FACILITY, et le message 200 OK associé à un message INVITE peut être remplacé par un message CONNECT.

L'invention décrite ici concerne un procédé et un serveur pour contrôler une communication sécurisée entre au moins deux terminaux par l'intermédiaire d'un serveur. Selon une implémentation de l'invention, les étapes du procédé de l'invention sont déterminées par les instructions d'un programme d'ordinateur incorporé dans un serveur, tel que le serveur de communication SC. Le programme comporte des instructions de programme, qui lorsque ledit programme est chargé et exécuté dans le dispositif, réalisent les étapes du procédé de l'invention.

En conséquence, l'invention s'applique également à un programme d'ordinateur, notamment un programme d'ordinateur sur ou dans un support d'informations, adapté à mettre en œuvre l'invention. Ce programme peut utiliser n'importe quel langage de programmation, et être sous la forme de code source, code objet, ou code intermédiaire entre code source et code objet tel que dans une forme partiellement compilée, ou dans n'importe quelle autre forme souhaitable pour implémenter le procédé selon l'invention.

REVENDICATIONS

1. Procédé pour contrôler une communication entre au moins un terminal sécurisé (TCs) et un terminal non sécurisé (TCns) par l'intermédiaire d'au moins un serveur (SC) à travers un réseau de télécommunications (RT), le terminal sécurisé (TCs) étant apte à transmettre et recevoir des flux de média chiffrés et le terminal non sécurisé (TCs) n'étant pas apte à transmettre et recevoir des flux de média chiffrés, comprenant dans le serveur (SC) :

suite à une réception (E1) d'un message (MesT) transmis depuis le terminal non sécurisé (TCns), le message (MesT) contenant une information indiquant que la communication entre le terminal non sécurisé (TCns) et le serveur (SC) n'est pas sécurisée,

une transmission (E2) d'un message (MesS) au terminal sécurisé (TCs), le message (MesS) contenant un paramètre de sécurité (Ps) indiquant que la communication entre le terminal sécurisé (TCs) et le terminal non sécurisé (TCns) n'est pas sécurisée.

2. Procédé conforme à la revendication 1, selon lequel le paramètre de sécurité (Ps) contenu dans le message (MesS) transmis au terminal sécurisé (TCs) est associé à un type de média, indiquant que le flux de média correspondant au type de média n'est pas chiffré.

3. Procédé conforme à la revendication 1 ou 2, selon lequel le paramètre de sécurité (Ps) contenu dans le message (MesS) transmis au terminal sécurisé (TCs) est associé à un type de chiffrement qui définit des caractéristiques d'un algorithme de chiffrement à utiliser pour chiffrer et déchiffrer un flux de média.

4. Procédé conforme à la revendication 1, selon lequel le paramètre de sécurité (Ps) contenu dans le message (MesS) transmis au terminal sécurisé (TCs) est associé à une indication sur le terminal non sécurisé (TCns) pour lequel la communication avec le serveur (SC) n'est pas sécurisée.

5. Procédé conforme à l'une des revendications 1 à 4, selon lequel les flux de média échangés lors de la communication sont conformes au protocole SIP.

6. Procédé conforme à l'une des revendications 1 à 5, selon lequel le message (MesS) transmis au terminal sécurisé (TCs) est l'un des messages de type "INVITE", "RE-INVITE", "200 OK", et "UPDATE" conformes au protocole SIP.

7. Procédé conforme à la revendication 6, selon lequel le paramètre de sécurité (Ps) contenu dans le message (MesS) transmis au terminal sécurisé (TCs) est inclus dans un en-tête dans ledit message (MesS).

8. Procédé conforme à la revendication 6, selon lequel le paramètre de sécurité (Ps) contenu dans le message (MesS) transmis au terminal sécurisé (TCs) est inclus dans un sous-message qui est encapsulé dans ledit message (MesS) et qui comporte des données utilisables par la couche transport.

9. Serveur pour contrôler une communication entre au moins un terminal sécurisé (TCs) et un terminal non sécurisé (TCns) par l'intermédiaire au moins du serveur (SC) à travers un réseau de télécommunications (RT), le terminal sécurisé (TCs) étant apte à transmettre et recevoir des flux de média chiffrés et le terminal non sécurisé (TCs) n'étant pas apte à transmettre et recevoir des flux de média chiffrés, comprenant :

des moyens (COM) pour transmettre un message (MesS) au terminal sécurisé (TCs), le message (MesS) contenant un paramètre de sécurité (Ps) indiquant que la communication entre le terminal sécurisé (TCs) et le terminal non sécurisé (TCns) n'est pas sécurisée, suite à une réception d'un message (MesT) transmis depuis le terminal non sécurisé (TCns), le message (MesT) contenant une information indiquant que la communication entre le terminal non sécurisé (TCns) et le serveur (SC) n'est pas sécurisée.

10. Programme d'ordinateur apte à être mis en œuvre dans un serveur (SC) pour contrôler une communication entre au moins un terminal sécurisé (TCs) et un terminal non sécurisé (TCns) par l'intermédiaire d'au moins un serveur (SC) à travers un réseau de télécommunications (RT), le terminal sécurisé (TCs) étant apte à transmettre et recevoir des flux de média chiffrés et le terminal non sécurisé (TCs) n'étant pas apte à transmettre et recevoir des flux de média chiffrés, ledit

programme comprenant des instructions qui, lorsque le programme est chargé et exécuté dans ledit serveur, réalisent les étapes suivantes :

suite à une réception (E1) d'un message (MesT) transmis depuis le terminal non sécurisé (TCns), le message (MesT) contenant une information indiquant que la communication entre le terminal non sécurisé (TCns) et le serveur (SC) n'est pas sécurisée,

une transmission (E2) d'un message (MesS) au terminal sécurisé (TCs), le message (MesS) contenant un paramètre de sécurité (Ps) indiquant que la communication entre le terminal sécurisé (TCs) et le terminal non sécurisé (TCns) n'est pas sécurisée.

1/2
FIG. 1

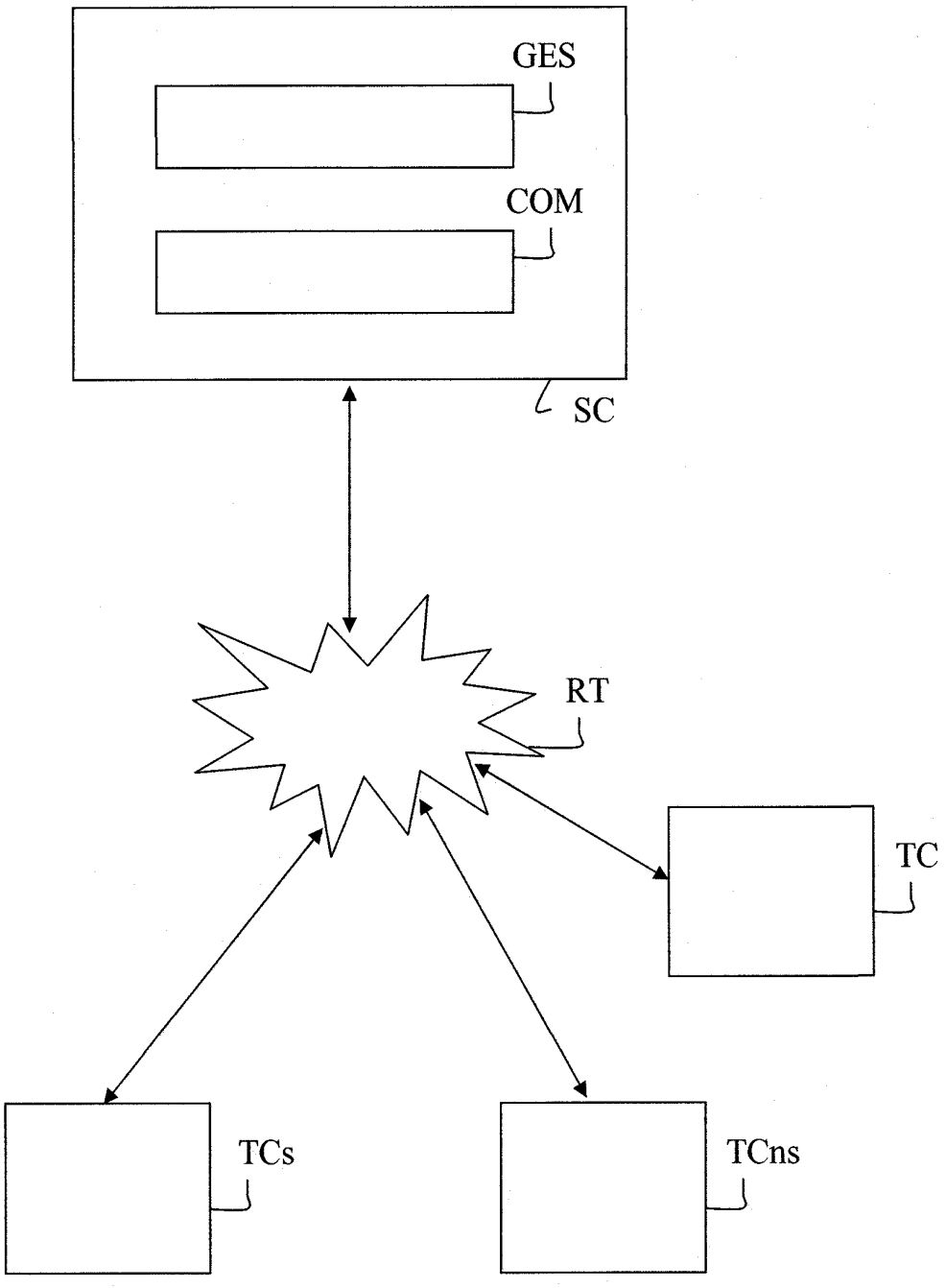
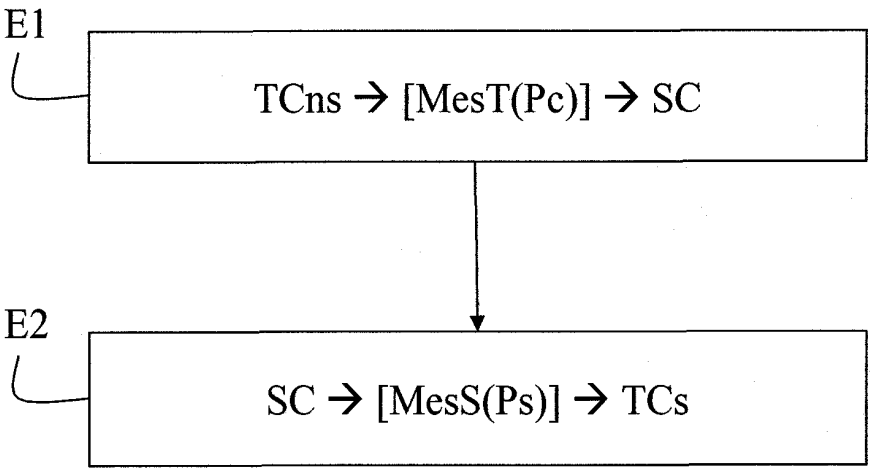


FIG. 2



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 740599
FR 1002772

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 2008/025516 A1 (MASUHIRO MAO [JP] ET AL) 31 janvier 2008 (2008-01-31) * alinéas [0019], [0027], [0216] - [0226]; figures 14,26 * -----	1-10	H04L29/06 H04L9/00
X	"LifeSize Video Communications Systems User Guide", LifeSize Communications Inc , novembre 2009 (2009-11), XP002619259, Extrait de l'Internet: URL:http://www.cs.washington.edu/lab/facilities/videoconferencing/administrator-guide_video_45_english.pdf [extrait le 2011-02-01] * page 24 * -----	1-10	
X	"LifeSize Video Communications Systems Administration Guide", LifeSize Communications Inc , novembre 2009 (2009-11), XP002619260, Extrait de l'Internet: URL:http://www.cs.washington.edu/lab/facilities/videoconferencing/administrator-guide_video_45_english.pdf [extrait le 2011-02-01] * page 26 * -----	1-10	DOMAINES TECHNIQUES RECHERCHÉS (IPC) H04L
X	US 2010/142707 A1 (HAN CHANG-MIN [KR] ET AL) 10 juin 2010 (2010-06-10) * alinéas [0043], [0044], [0056] - [0065]; figures 1,3-4 * -----	1-10	

Date d'achèvement de la recherche	Examinateur
9 février 2011	Ghomrasseni, Z

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 1002772 FA 740599

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 09-02-2011
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 2008025516 A1	31-01-2008	AU 2007203552 A1	14-02-2008
		CN 101155188 A	02-04-2008
		GB 2440653 A	06-02-2008
		JP 4267008 B2	27-05-2009
		JP 2008035235 A	14-02-2008
		NL 1034193 A1	29-01-2008
US 2010142707 A1	10-06-2010	KR 20100064585 A	15-06-2010

EPO FORM P0465