La domotique et la sécurité des biens et des personnes

Le brevet :
Déposé en 2001, ce brevet à fait l'objet d'une délivrance par l'INPI en 2003.

Le déposant :
Possédant une expérience de plusieurs années dans le bâtiment (courants forts, courants faibles, navaids, …), expert de la sécurité et de la confidentialité des échanges sur Internet, spécialiste des échanges dématérialisés, du BtoB et des NTIC, le déposant possède plusieurs brevets dont l'un, datant de 1988, à fait l'objet d'une industrialisation commercialisée à plusieurs millions d'exemplaires.

Les enjeux du brevet :
Le brevet permet d'apporter une solution domotique utilisant le réseau Internet et répondant aux critères suivants :
- usage simple et pratique ;
- utilisation d'un moyen de communication économique ;
- fiabilité du support de transmission ;
- identification de l'utilisateur ;
- sécurisation des informations ;
- confidentialité des informations personnelles ;
- …

Titre du brevet :
Système de sécurisation de l'authentification d'informations émises à travers un réseau de transmission d'informations / System for secure authentication of information transmitted across a data network, comprising microcomputer and authentication terminal connected via a switch with a controller to a modem and the network.

Références du brevet :
No. Publication (Sec.) : FR2826533
Date de publication : 2002-12-27
Numéro original : FR2826533
No. d`enregistrement : FR20010008127 20010620
No. de priorité : FR20010008127 20010620
Classification IPC : H04L12/22; H04L9/00; G06F13/14
Classification EC : H04L29/06C6, H04L29/06C6C2
Classification EC : H04L29/06C6; H04L29/06C6C2
Brevets correspondants : -

Abrégé du brevet :
System for secure authentication of information transmitted across a data network, whereby the system comprises a microcomputer (3) connected to a network (1) via a modem (4). Also connected to the modem is an authentication terminal (5). Between terminal and microcomputer and the modem is a switch (7) with a controller (8). The controller commands the switch such that only the microcomputer or the authentication terminal are connected at any one time.

Description du brevet :
La présente invention concerne un système de sécurisation de l'authentification d'informations émises à travers un réseau de transmission d'informations.

On a assisté depuis quelques années à une augmentation très importante des échanges d'informations en ligne.

Ces échanges sont en fait basés sur la circulation d'informations à travers des réseaux de transmission d'informations notamment entre des centres serveurs et des terminaux de traitement d'informations comportant par exemple des micro-ordinateurs permettant à chaque utilisateur de recevoir des informations.

Ces micro-ordinateurs sont alors associés à des moyens formant modulateur/démodulateur également appelés modems, pour assurer leur raccordement au réseau de transmission d'informations.

L'un des problèmes liés à l'utilisation de tels réseaux réside dans le fait que l'origine des informations n'est pas certaine. Pour tenter de résoudre ces problèmes, on a alors proposé d'utiliser des terminaux d'authentification des informations émises.

Ces terminaux comprennent alors par exemple des moyens d'identification morphologique, de signature électronique, etc..., permettant d'une certaine façon à l'utilisateur de certifier l'origine des informations.

Ces terminaux d'authentification sont alors intégrés directement à l'un des éléments du micro-ordinateur, comme par exemple le clavier, la souris ou encore le carter d'écran de celui-ci.

Des boîtiers indépendants se présentant par exemple sous la forme d'un périphérique externe aux micro-ordinateurs, ont également été envisagés.

Le problème de ces structures réside dans le fait que ces terminaux sont associés aux micro-ordinateurs et plus particulièrement à l'unité centrale de ceux-ci, de sorte qu'ils peuvent facilement être piratés à travers le réseau.

En effet, on sait que l'accès à distance à un micro-ordinateur à travers un réseau de transmission d'informations est relativement simple à mettre en oeuvre, pour accéder aux ressources de celui-ci et en particulier au terminal d'authentification à travers l'unité centrale du micro-ordinateur, ce qui permet de le pirater.

Le but de l'invention est donc de résoudre ces problèmes.

A cet effet, l'invention a pour objet un système d'authentification d'informations émises à travers un réseau de transmission d'informations, du type comportant des moyens formant micro-ordinateur raccordés au réseau de transmission d'informations à travers des moyens formant modulateur/démodulateur et des moyens formant terminal d'authentification, caractérisé en ce que les moyens formant micro-ordinateur et les moyens formant terminal d'authentification, sont reliés aux moyens formant modulateur/démodulateur, de façon distincte, à travers des moyens formant basculeur commandés par des moyens de pilotage pour connecter de façon exclusive l'un ou l'autre de ces moyens aux moyens formant modulateur/démodulateur.

Selon d'autres caractéristiques : - les moyens de pilotage comprennent des moyens de reconnaissance d'ordres de commande de basculement dans les signaux circulant entre les moyens formant micro-ordinateur, les moyens formant terminal d'authentification et les moyens formant modulateur/démodulateur ; - les moyens formant micro-ordinateur sont adaptés pour émettre un ordre de basculement pour connecter les moyens formant terminal d'authentification afin de déclencher une phase d'authentification et les moyens formant terminal d'authentification sont adaptés pour émettre un ordre de bascule ment pour connecter les moyens formant micro-ordinateur afin de

terminer l'opération d'authentification ; - les moyens formant modulateur/démodulateur, les moyens de basculement et les moyens de pilotage de ceux-ci, sont intégrés dans un même boîtier sécurisé, indépendant des moyens formant micro-ordinateur et des moyens formant terminal d'authentification.

L'invention sera mieux comprise à la lecture de la description qui va suivre, donnée uniquement à titre d'exemple et faite en se référant aux dessins annexés, sur lesquels : - la Fig. 1 représente un schéma synoptique illustrant la structure générale d'un système selon l'invention ; et - la Fig. 2 illustre un organigramme de fonctionnement de celui-ci.

On a en effet représenté sur la figure 1, un système de sécurisation de l'authentification d'informations émises à travers un réseau de transmission d'informations.

Le réseau de transmission d'informations est désigné par la référence générale 1 et est par exemple formé par un réseau téléphonique accessible à travers une prise de raccordement désignée par la référence générale 2, de façon classique.

Dans le système selon l'invention, il est également prévu des moyens formant micro-ordinateur désignés par la référence générale 3 sur cette figure, comportant de façon classique, par exemple un clavier, une souris, une unité centrale et un écran d'affichage d'informations, etc...

Ces moyens formant micro-ordinateur sont raccordés au réseau de transmission d'informations à travers des moyens formant modulateur/démodulateur désignés par la référence générale 4 et présentant n'importe quelle structure appropriée.

Le système selon l'invention comporte également des moyens formant terminal d'authentification désignés par la référence générale 5 de type classique, adaptés pour recevoir par exemple une carte à mémoire désignée par la référence générale 6, de type carte à puce, etc...

Différents types de terminaux d'authentification peuvent être envisagés, de façon classique.

Dans l'exemple décrit, ce terminal est associé à une carte à mémoire et dispose par exemple d'un clavier d'entrée de code confidentiel par l'utilisateur.

Selon l'invention, les moyens formant micro-ordinateur et les moyens formant terminal d'authentification sont reliés aux moyens formant modulateur/démodulateur, de façon distincte, à travers des moyens formant basculeur désignés par la référence générale 7 sur cette figure, et commandés par des moyens de pilotage désignés par la référence générale 8, pour connecter de façon exclusive, l'un ou l'autre de ces moyens aux moyens formant modulateur/démodulateur 4.

En fait, les moyens de pilotage 8 peuvent comporter des moyens de reconnaissance d'ordres de commande de basculement dans les signaux circulant entre les moyens formant micro-ordinateur, les moyens formant terminal d'authentification et les moyens formant modulateur/démodulateur.

Les moyens formant basculeur peuvent présenter n'importe quelle structure appropriée, par exemple à commutateur à semi-conducteur piloté.

Les moyens de pilotage et de reconnaissance peuvent quant à eux par exemple être formés par des moyens logiciels de contrôle.

Le fonctionnement d'un tel système est illustré sur la figure 2.

Lorsqu'un opérateur utilisant les moyens formant micro-ordinateur 3 échange des informations par exemple avec un centre-serveur lors d'une étape désignée par la référence générale 10 sur cette figure 2, il peut par exemple procéder à l'authentification des informations qu'il transmet au centre.

Dans ce cas, les moyens de basculement 7 sont dans la position illustrée sur la figure 1, c'est-à-dire que les moyens formant micro-ordinateur 3 sont raccordés aux moyens formant modulateur/démodulateur 4 et de là, au reste du réseau de transmission d'informations et au centre-serveur.

Lorsque l'opérateur souhaite déclencher l'authentification d'informations, il lance une opération d'authentification, par exemple lors de l'étape 11, par une action quelconque sur des moyens d'entrée de ces moyens formant micro-ordinateur, comme par exemple en enfonçant une touche correspondante ou en activant un pictogramme sur l'écran, etc...

Les moyens formant micro-ordinateur lancent alors une opération d'authentification en envoyant un ordre de basculement correspondant à destination des moyens de reconnaissance 8, comme cela est illustré par l'étape désignée par la référence générale 12 sur cette figure 2.

Lors de la reconnaissance de cet ordre de basculement, les moyens 8 déclenchent le pilotage des moyens de basculement 7 pour que ceux-ci basculent dans l'autre position, afin de raccorder les moyens formant terminal d'authentification 5 au reste du circuit et de couper la connexion des moyens formant micro-ordinateur 3, comme cela est illustré par l'étape 13.

L'opérateur peut alors effectuer l'authentification des informations en utilisant de façon classique, les moyens formant terminal d'authentification 5 en y introduisant par exemple la carte à mémoire 6 et en composant son code confidentiel.

Ces informations d'authentification sont alors utilisées de façon classique par le centre-serveur.

D'autres terminaux d'authentification par identification morphologique, signature électronique, etc..., de l'utilisateur peuvent bien entendu être envisagés.

Une fois l'opération d'authentification effectuée, comme cela est illustré par l'étape 14, le terminal d'authentification émet un ordre de fin d'opération d'authentification lors par exemple d'une étape désignée par la référence générale 15.

Cet ordre est alors détecté par les moyens de reconnaissance 8 qui déclenchent lors de l'étape 16, le basculement des moyens de basculement 7 vers la position illustrée sur la figure 1, en coupant la connexion des moyens formant terminal d'authentification 5, tout en assurant la connexion des moyens formant micro-ordinateur 3, au reste du circuit.

Il va de soi bien entendu que des échanges d'informations complémentaires de type classique, sont mis en oeuvre entre les moyens formant micro ordinateur, les moyens formant terminal d'authentification et le centre-serveur, pour assurer la transmission des informations correspondantes, de façon classique.

On conçoit alors que grâce à une telle structure, il n'est pas possible d'avoir accès aux ressources des moyens formant terminal d'authentification à travers l'unité centrale des moyens formant micro-ordinateur, dans la mesure où ceux-ci sont reliés de façon distincte aux moyens formant modulateur/démodulateur, à travers les moyens formant basculeur, qui sont commandés pour connecter de façon exclusive l'un ou l'autre de ces moyens à ces moyens formant modulateur/démodulateur.

Selon un mode de réalisation, les moyens de basculement 7, les moyens de pilotage 8 et les moyens formant modulateur/démodulateur 4, sont intégrés dans un seul et même boîtier sécurisé désigné par la référence générale 17 sur la figure 1, ce boîtier étant indépendant des moyens formant micro ordinateur et des moyens formant terminal d'authentification et étant sécurisé de façon classique par exemple par des moyens d'effacement de mémoire à l'ouverture de ce boîtier.

Revendications

1. Système de sécurisation de l'authentification d'informations émises à travers un réseau de transmission d'informations (1), du type comportant des moyens (3) formant micro-ordinateur raccordés au réseau de transmission d'informations (1) à travers des moyens formant modulateur/démodulateur (4) et des moyens (5) formant terminal d'authentification (6), caractérisé en ce que les moyens formant micro-ordinateur (3) et les moyens formant terminal d'authentification (5) sont reliés aux moyens formant modulateur/démodulateur (4), de façon distincte, à travers des moyens formant basculeur (7), commandés par des moyens de pilotage (8) pour connecter de façon exclusive l'un ou l'autre de ces moyens aux moyens formant modulateur/démodulateur.

2. Système selon la revendication 1, caractérisé en ce que les moyens de pilotage (8) comprennent des moyens de reconnaissance d'ordres de commande de basculement dans les signaux circulant entre les moyens formant micro-ordinateur (3), les moyens formant terminal d'authentification (5) et les moyens formant modulateur/démodulateur (4).

3. Système selon l'une quelconque des revendications précédentes, caractérisé en ce que les moyens formant micro-ordinateur (3) sont adaptés pour émettre un ordre de basculement pour connecter les moyens formant terminal d'authentification (5) afin de déclencher une phase d'authentification et en ce que les moyens formant terminal d'authentification (5), sont adaptés pour émettre un ordre de basculement pour connecter les moyens formant micro-ordinateur (3) afin de terminer l'opération d'authentification.

4. Système selon l'une quelconque des revendications précédentes, caractérisé en ce que les moyens formant modulateur/démodulateur (4), les moyens de basculement (7) et les moyens de pilotage de ceux-ci (8), sont intégrés dans un même boîtier sécurisé (17), indépendant des moyens formant micro-ordinateur (3) et des moyens formant terminal d'authentification (5).

Schéma :

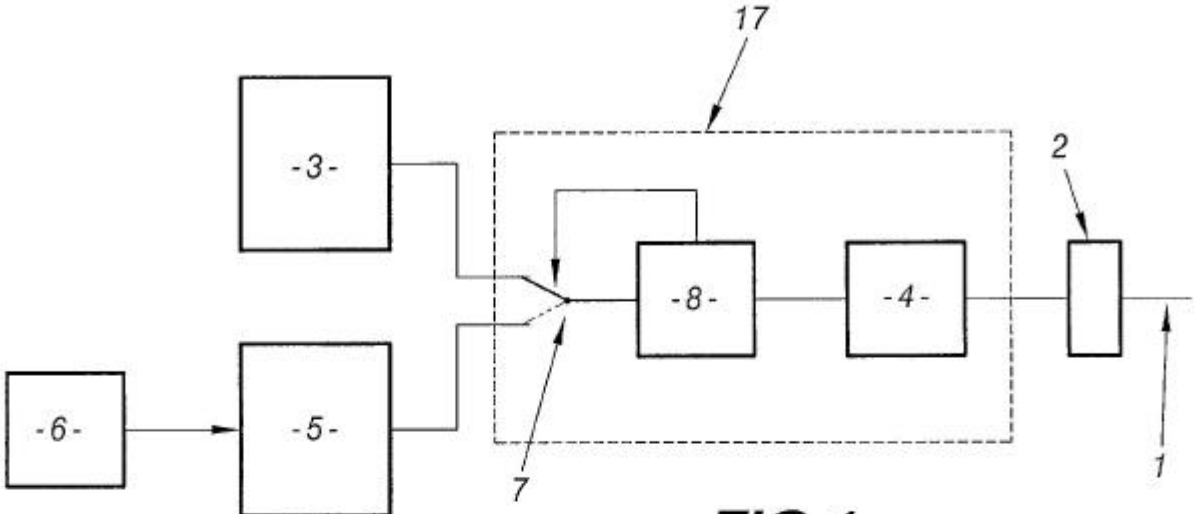

FIG.1

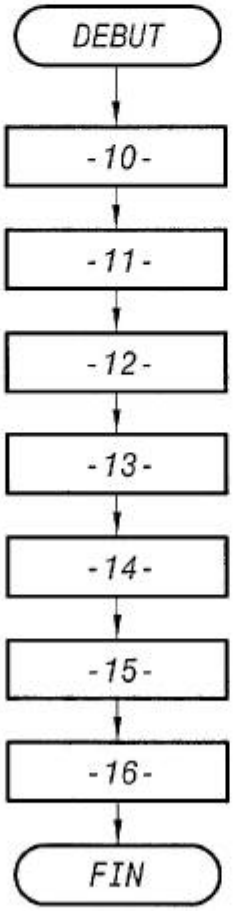

FIG.2