(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
6 janvier 2011 (06.01.2011)

PCT

(10) Numéro de publication internationale
WO 2011/000756 A1

(51) Classification internationale des brevets :
G06F 21/00 (2006.01) *G06F 21/02* (2006.01)

(21) Numéro de la demande internationale :
PCT/EP2010/058949

(22) Date de dépôt international :
23 juin 2010 (23.06.2010)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0954431 29 juin 2009 (29.06.2009) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **VIACCESS** [FR/FR]; Les Collines de l'Arche, Tour Operera C, F-92057 Paris La Défense (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **BARAU, Emmanuel** [FR/FR]; 44 rue Albert Joly, F-78000 Versailles (FR). **GRANET, Olivier** [FR/FR]; 1 rue des Cottages, F-92150 Suresnes (FR). **SOCQUET, Patrick** [FR/FR]; 24 rue de Pontoise, F-75005 Paris (FR).

(74) Mandataires : **COLOMBO, Michel** et al.; 324 rue Garibaldi, F-69007 Lyon (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Suite sur la page suivante]

(54) **Title** : METHOD FOR DETECTING AN ATTEMPTED ATTACK, RECORDING MEDIUM, AND SECURITY PROCESSOR FOR SAID METHOD

(54) **Titre** : PROCEDE DE DETECTION D'UNE TENTATIVE D'ATTAQUE, SUPPORT D'ENREGISTREMENT ET PROCESSEUR DE SECURITE POUR CE PROCEDE

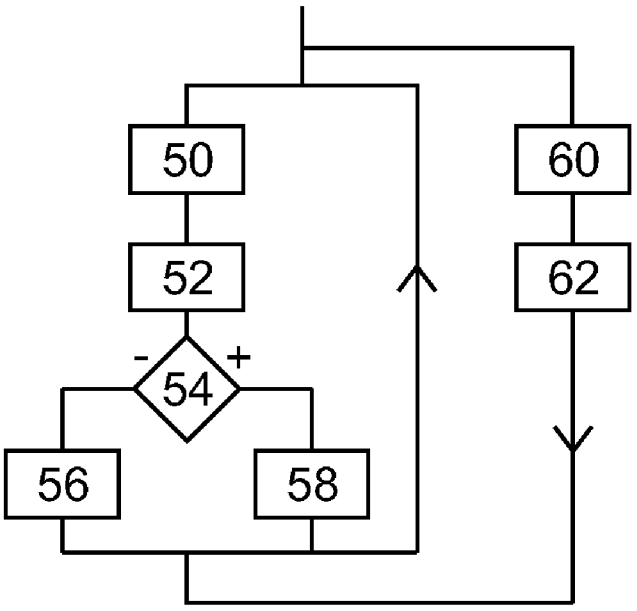

Fig. 4

(57) **Abstract** : The invention relates to a method for detecting an attempted attack of a security processor by the security processor itself, including: measuring (50) a plurality of separate events taking place independently of one another in the absence of an attempted attack; constructing (52) the value of at least one attack indicator in accordance with at least one concomitance index between at least two separate measured events, the concomitance index representing the proximity in time of the two separate measured events; and detecting (54) an attempted attack if the value of the attack indicator exceeds a predetermined threshold.

(57) **Abrégé** : Ce procédé de détection d'une tentative d'attaque d'un processeur de sécurité par le processeur de sécurité lui-même, comprend : des mesures (50) de plusieurs événements différents se produisant indépendamment les uns des autres en absence de tentative d'attaque, la construction (52) de la valeur d'au moins un indicateur d'attaque en fonction d'au moins un indice de concomitance entre au moins deux événements différents mesurés, l'indice de concomitance étant représentatif de la proximité temporelle entre les deux événements différents mesurés, et la détection (54) d'une tentative d'attaque si la valeur de l'indicateur d'attaque franchit un seuil prédéterminé.

WO 2011/000756 A1

Publiée :

— *avec rapport de recherche internationale (Art. 21(3))*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues (règle 48.2.h))*

PROCEDE DE DETECTION D'UNE TENTATIVE D'ATTAQUE, SUPPORT D'ENREGISTREMENT ET PROCESSEUR DE SECURITE POUR CE PROCEDE

[0001] L'invention concerne un procédé de détection d'une tentative d'attaque d'un processeur de sécurité par le processeur de sécurité lui-même. L'invention a également pour objet un support d'enregistrement d'informations ainsi qu'un processeur de sécurité pour la mise en œuvre de ce procédé.

[0002] Les processeurs de sécurité sont, généralement, des composants matériels renfermant des informations confidentielles telles que des clés cryptographiques ou des droits d'accès que seuls des utilisateurs légitimes peuvent utiliser. Pour préserver la confidentialité de ces informations, ils sont conçus pour être le plus robuste possible vis-à-vis de tentatives d'attaque menées par des pirates informatiques. Par exemple, un processeur de sécurité est une carte à puce équipée d'un processeur électronique.

[0003] Les processeurs de sécurité sont soumis à différents types d'attaque. Certaines de ces attaques visent à extraire ou à déterminer les informations confidentielles contenues dans le processeur de sécurité. A cet effet, une multitude d'attaques ont été développées. Par exemple certaines de ces attaques cherchent à obtenir un fonctionnement anormal du processeur de sécurité en lui faisant traiter des messages construits par les pirates informatiques. D'autres procédés plus invasifs cherchent à perturber le fonctionnement du processeur de sécurité à des moments clé de son fonctionnement en jouant sur sa tension d'alimentation ou encore à l'aide d'un faisceau laser dirigé vers le processeur de sécurité.

[0004] D'autres types d'attaque ne cherchent pas à extraire ou à déterminer des informations confidentielles contenues dans le processeur de sécurité mais consistent simplement à utiliser de façon abusive ce processeur de sécurité. Par exemple, dans le domaine de la télévision payante, la redistribution de mots de contrôle (ou « control word sharing » en anglais) et le partage de carte (« card sharing » en anglais) rentrent dans ce type d'attaque. Sommairement, la redistribution de mots de contrôle consiste à distribuer le mot de contrôle déchiffré par le processeur de sécurité vers plusieurs récepteurs. Ces récepteurs peuvent alors déchiffrer les contenus multimédias embrouillés avec ce mot de contrôle alors que l'abonnement n'a été souscrit et payé que pour un seul récepteur.

[0005] Le partage de carte consiste à faire déchiffrer par un même processeur de sécurité plusieurs mots de contrôle chiffrés provenant de différents récepteurs. Comme précédemment, tous ces récepteurs peuvent alors désembrouiller les contenus multimédias embrouillés alors qu'un seul de ces récepteurs est habilité à accéder au contenu.

[0006] Pour lutter contre ces attaques, il est connu de détecter les tentatives d'attaque et, en réponse à cette détection, d'exécuter une contre-mesure.

[0007] Un exemple de procédé de détection de tentative d'attaque et d'exécution, en réponse, de contre-mesure est par exemple décrit dans la demande de brevet EP 1 575 293.

[0008] La contre-mesure est une action qui vise à empêcher que l'attaque contre le processeur de sécurité ne puisse perdurer ou ne puisse être fructueuse. Il existe un grand nombre de contre-mesures exécutables par un processeur de sécurité. Celles-ci vont d'un simple accroissement des mesures de sécurité dans le processeur de sécurité jusqu'à un blocage définitif et irrémédiable du processeur de sécurité qui devient alors inutilisable.

[0009] Pour détecter une tentative d'attaque, il a déjà été proposé des procédés comprenant :

- des mesures de plusieurs événements différents se produisant indépendamment les uns des autres en absence de tentative d'attaque, puis
- de comparer chaque mesure à un seuil prédéterminé respectif pour détecter la présence ou l'absence d'une tentative d'attaque.

[0010] Toutefois, la difficulté vient du fait que les événements représentatifs d'une tentative d'attaque peuvent aussi se produire en absence de tentative d'attaque. Or, il faut éviter de produire de fausses détections de tentative d'attaque car celles-ci peuvent se traduire par l'exécution intempestive de contre-mesures qui gênent alors l'utilisateur légitime du processeur de sécurité. Pour cette raison, il est connu de choisir pour le seuil prédéterminé une valeur beaucoup plus élevée que toutes les mesures qui peuvent être obtenues en absence d'attaque. Toutefois, le choix d'un seuil prédéterminé élevé rend certaines attaques indétectables ou ralentit la détection d'une tentative d'attaque.

[0011] L'invention vise à remédier à ce problème en proposant un procédé de détection d'une tentative d'attaque comportant également :

- la construction de la valeur d'au moins un indicateur d'attaque en fonction d'au moins un indice de concomitance entre au moins deux événements différents mesurés, l'indice de concomitance étant représentatif de la proximité temporelle entre les deux événements différents mesurés, et
- la détection d'une tentative d'attaque si la valeur de l'indicateur d'attaque franchit un seuil prédéterminé.

[0012] Le procédé ci-dessus prend en compte la proximité temporelle entre différents événements survenant dans le processeur de sécurité. Cela permet de détecter plus rapidement une tentative d'attaque ou de détecter une tentative d'attaque qui ne pourrait pas être détectée par l'observation de la mesure d'un seul événement. En effet, pris individuellement, la mesure de chacun de ces événements peut ne pas être rapidement représentative d'une tentative d'attaque puisque ces événements se produisent lors d'un fonctionnement normal du processeur de sécurité. Par contre, lorsque ces événements se produisent quasiment

concomitamment alors que normalement ils doivent se produire indépendamment les uns des autres, cela indique, avec un fort degré de confiance, qu'une tentative d'attaque a lieu. Le procédé ci-dessus permet donc au processeur de sécurité de détecter rapidement et avec un grand degré de confiance qu'il est victime d'une tentative d'attaque. L'exécution des contre-mesures appropriées peut alors être déclenchée plus rapidement.

[0013] Les modes de réalisation de ce procédé peuvent comporter une ou plusieurs des caractéristiques suivantes :

- la valeur de l'indicateur d'attaque est construite à partir de plusieurs indices de concomitance entre des événements différents mesurés et en pondérant l'importance de ces indices de concomitance les uns par rapport aux autres à l'aide d'un jeu prédéterminé de coefficients de pondération ;
- le procédé comprend la construction de plusieurs valeurs d'indicateurs d'attaque en utilisant plusieurs jeux différents de coefficients de pondération entre les mêmes indices de concomitance, chaque jeu de coefficients de pondération étant prédéterminé pour être plus sensible à une tentative d'attaque différente de celles auxquelles sont plus sensibles les autres indicateurs ;
- le coefficient de pondération d'un même indice de concomitance est le même dans tous les jeux de coefficients de pondération utilisés pour construire les différentes valeurs d'indicateurs d'attaque
- la mesure d'un événement est limitée à une fenêtre temporelle glissante de manière à ne pas prendre en compte des événements qui se sont produits en dehors de cette fenêtre temporelle, ceci pour établir que les événements sont concomitants dans la mesure de cette fenêtre temporelle;
- au moins l'un des événements mesurés est la détection d'une erreur de fonctionnement du processeur de sécurité dont chaque occurrence conduit le processeur de sécurité à arrêter les traitements en cours et à se réinitialiser automatiquement pour reprendre ces traitements depuis le début ;
- la mesure d'un événement consiste à comptabiliser dans un compteur le nombre de fois où cet événement s'est produit, la valeur du compteur constituant la mesure
- l'indice de concomitance entre au moins deux mesures est obtenu en multipliant entre elles ces mesures.

[0014] Ces modes de réalisation du procédé présentent en outre les avantages suivants :

- l'utilisation de coefficients de pondération entre les indices de concomitance permet de modifier simplement la sensibilité de l'indicateur d'attaque construit à un type particulier d'attaque en modifiant la valeur de ces coefficients de pondération,

- l'utilisation de plusieurs jeux différents de coefficients de pondération permet, à partir du même jeu d'indices de concomitance, de construire plusieurs indicateurs d'attaque chacun dédiés à la détection d'une tentative d'attaque différente,
- l'utilisation systématique du même coefficient de pondération pour le même indice de concomitance permet de limiter la quantité de mémoire requise pour stocker ces différents coefficients de pondération,
- limiter la mesure d'un événement à une fenêtre temporelle glissante permet de limiter le nombre de fausses détections de tentative d'attaque causées par l'accumulation dans le temps d'événements mesurés en absence de tentative d'attaque,
- lorsque l'un des événements mesurés est la détection d'une erreur du processeur de sécurité provoquant la réinitialisation de ce processeur de sécurité, la sécurité est accrue en empêchant le blocage intempestif du processeur de sécurité.

[0015] L'invention a également pour objet un support d'enregistrement d'informations comportant des instructions pour l'exécution du procédé ci-dessus, lorsque ces instructions sont exécutées par un calculateur électronique.

[0016] Enfin, l'invention a également pour objet un processeur de sécurité comportant :

- des registres dans lesquels sont stockées des mesures de plusieurs événements se produisant indépendamment les uns des autres en absence de tentative d'attaque, et
- un calculateur, apte :
  - à construire la valeur d'au moins un indicateur d'attaque en fonction d'au moins un indice de concomitance entre au moins deux événements différents mesurés dont les mesures sont stockées dans les registres, cet indice de concomitance étant représentatif de la proximité temporelle entre les deux événements différents mesurés, et
  - à détecter une tentative d'attaque si la valeur de l'indicateur d'attaque franchit un seuil prédéterminé.

[0017] L'invention sera mieux comprise à la lecture de la description qui va suivre, donnée uniquement à titre d'exemple non limitatif et faite en se référant aux dessins sur lesquels :

- la figure 1 est une illustration schématique d'un système de transmission de contenus multimédias embrouillés comportant un processeur de sécurité,
- la figure 2 est une illustration schématique d'une matrice de coefficients de pondération utilisée par le processeur de sécurité du système de la figure 1,
- la figure 3 est une illustration schématique d'une table de seuils d'alerte utilisée par le processeur de sécurité de la figure 1, et

- la figure 4 est un organigramme d'un procédé de détection d'une tentative d'attaque du processeur de sécurité du système de la figure 1.

[0018] Sur ces figures, les mêmes références sont utilisées pour désigner les mêmes éléments.

[0019] Dans la suite de cette description, les caractéristiques et fonctions bien connues de l'homme du métier ne sont pas décrites en détail. De plus, la terminologie utilisée est celle des systèmes d'accès conditionnel à des contenus multimédias. Pour plus d'informations sur cette terminologie, le lecteur peut se reporter au document suivant :

« *Functional model of a conditional access system* » EBU Review – Technical european broadcasting union, Brussels, BE, n° 266, 21 décembre 1995.

[0020] La figure 1 représente un système de diffusion payante de contenus multimédias. Par exemple, le système 2 est un système permettant de diffuser plusieurs chaînes de télévision embrouillées. Le désembrouillage de chacune de ces chaînes de télévision ou groupe de chaînes de télévision est conditionné au paiement d'un abonnement par des abonnés. Dans cette description, les termes « embrouiller »/« chiffrer » et « désembrouiller »/ « déchiffrer » sont considérés comme synonymes.

[0021] Le système 2 comprend au moins un émetteur 4 de contenus multimédias embrouillés et une multitude de récepteurs aptes à désembrouiller le contenu multimédia diffusé par l'émetteur 4. Pour simplifier la figure 1, seul un récepteur 6 a été représenté. Par exemple, les autres récepteurs sont identiques au récepteur 6.

[0022] Le récepteur 6 est raccordé à l'émetteur 4 par l'intermédiaire d'un réseau 8 grande distance de transmission d'informations. Le réseau 8 peut être un réseau de télécommunication sans fil ou un réseau filaire tel qu'Internet.

[0023] Typiquement, l'émetteur 4 diffuse les contenus multimédias embrouillés multiplexés avec des messages de contrôle ECM (Entitlement Control Message) et EMM (Entitlement Management Message). Chaque message ECM comprend au moins un cryptogramme CW* d'un mot de contrôle CW permettant de désembrouiller le contenu multimédia embrouillé.

[0024] Le récepteur 6 comprend un décodeur 10 et un processeur de sécurité 12 raccordé de façon amovible au décodeur 10.

[0025] Le décodeur 10 comprend un récepteur 14 des données transmises par l'émetteur 4 raccordé à un démultiplexeur 16. Le démultiplexeur 16 démultiplexe les données reçues et transmet le contenu multimédia embrouillé à un désembrouilleur 18 et les messages ECM ou EMM au processeur de sécurité 12.

[0026] Le processeur 12 reçoit le cryptogramme CW* et déchiffre ce cryptogramme afin de renvoyer le mot de contrôle CW en clair au désembrouilleur 18. Ce déchiffrement n'est autorisé que si les titres d'accès contenus dans le message ECM

correspondent à des droits d'accès mémorisés dans le processeur de sécurité 12. Par exemple, le processeur 12 est le processeur d'une carte à puce.

[0027] Le désembrouilleur 18 désembrouille le contenu multimédia embrouillé à l'aide du mot de contrôle CW déchiffré par le processeur de sécurité 12. Le contenu multimédia désembrouillé est alors, par exemple, affiché en clair sur un écran 20 de manière à ce que le contenu multimédia affiché soit directement perceptible et compréhensible par l'utilisateur.

[0028] Les fonctions et les caractéristiques du processeur 12 pour réaliser les différentes opérations liées au déchiffrement des mots de contrôle CW sont connues et ne sont pas décrites ici plus en détail.

[0029] Le processeur 12 comporte un calculateur électronique 24 raccordé à des capteurs 26, 27 et à un ensemble 30 de registres.

[0030] Le capteur 26 comprend un transducteur de tension apte à convertir la tension d'alimentation du processeur 12 en une donnée numérique exploitable par le calculateur 24.

[0031] Le capteur 27 comprend un transducteur de lumière apte à convertir des photons d'un faisceau laser dirigé sur le processeur 12 en données numériques exploitables par le calculateur 24.

[0032] A titre d'illustration, l'ensemble 30 comprend onze registres référencés C_0 à C_{10}. Chacun des registres C_1 à C_{10} est destiné à contenir une mesure d'un événement qui peut être déclenché par une tentative d'attaque du processeur 12. Les événements mesurés peuvent également se produire en absence de tentative d'attaque. Toutefois, en absence de tentative d'attaque ces événements mesurés se produisent indépendamment les uns des autres. Ainsi, il est peut probable qu'en absence de tentative d'attaque, les événements mesurés se produisent concomitamment. Par concomitamment, on désigne le fait qu'ils se produisent pendant une même fenêtre temporelle. Ici, une fenêtre temporelle est associée à chaque événement mesuré. Cette fenêtre temporelle peut avoir une durée finie ou, au contraire, infinie. Dans le cas d'une durée finie, cela signifie que les événements qui se produisent en dehors de cette fenêtre temporelle ne sont pas pris en compte dans la mesure de cet événement. Ici, une fenêtre temporelle de durée finie est une fenêtre temporelle glissante. Cette fenêtre temporelle glissante a une durée finie que l'on décale au fur et à mesure que le temps s'écoule pour ne prendre en compte que les événements les plus récents pour la mesure de cet événement. Une durée infinie signifie que tous les événements sont pris en compte pour la mesure depuis que la mesure de cet événement a été déclenchée.

[0033] Ici, la mesure d'un événement consiste à compter le nombre de fois où cet événement s'est produit pendant la fenêtre temporelle associée à cet événement. Ainsi, chacun des registres contient un nombre représentatif du nombre

d'occurrences d'un même événement. Par conséquent, dans la suite de cette description, les registres C_i sont appelés compteurs C_i.

[0034] Il existe un grand nombre d'événements mesurables. Typiquement, les événements mesurés rentrent dans l'une des catégories suivantes :

- des événements normaux qu'un utilisateur légitime peut déclencher mais qui, s'ils se produisent en grand nombre, sont représentatifs d'une utilisation anormale du processeur 12,
- la réception par le processeur 12 de messages erronés ou inutiles, c'est-à-dire de messages qui ne devraient pas exister lors d'une utilisation normale et dépourvue d'erreur,
- la détection d'erreurs de fonctionnement du processeur 12.

[0035] Il existe de nombreuses erreurs de fonctionnement. Par exemple, les erreurs de fonctionnement peuvent être des erreurs dans l'exécution du code du système d'exploitation du processeur 12, la mesure par les capteurs 26 ou 27 d'une situation anormale, la découverte d'erreur d'intégrité sur des données traitées, ...etc. Généralement, en cas de détection d'erreur de fonctionnement, les traitements en cours sont interrompus et le processeur 12 se réinitialise automatiquement.

[0036] Nous détaillons maintenant, pour chaque compteur, un exemple d'événement mesuré.

[0037] Le compteur C_1 contient le nombre de fois où une commande de consultation des données du processeur 12 a été reçue. En effet, un certain nombre de données contenues dans le processeur 12 sont librement consultables. Par exemple, il existe des commandes pour consulter le numéro d'identification du processeur 12 ou des droits d'accès enregistrés dans le processeur 12. La réception d'une commande de consultation est donc un événement normal tant que cela reste occasionnel. Par contre, le dénombrement d'un grand nombre de commandes de consultation de données du processeur 12 sur un bref intervalle de temps peut être provoqué par une tentative d'attaque.

[0038] Le compteur C_2 indique la présence de droits inhabituels inscrits dans le processeur 12. Un droit inhabituel est un droit que l'opérateur du système 2 n'utilise normalement pas. Par exemple, la plupart des opérateurs n'inscrivent jamais dans les processeurs de sécurité un droit dont la durée de validité est supérieure à un an. Dès lors, un droit inscrit dans le processeur 12 dont la durée de validité est supérieure à un an, par exemple un droit de durée de validité infinie, est un droit inhabituel même si cette possibilité est techniquement prévue. De façon similaire, normalement, l'opérateur n'inscrit jamais un droit autorisant l'accès et le déchiffrement de tous les contenus multimédias dans les processeurs de sécurité. Dans ces conditions, l'inscription d'un droit autorisant l'accès à tous ces contenus multimédias dans le processeur 12 est considérée comme un droit inhabituel. L'inscription d'un droit

inhabituel dans le processeur 12 peut provenir d'une erreur de l'opérateur mais peut également être représentative d'une tentative d'attaque.

[0039] Le compteur C_3 dénombre le nombre de messages reçus par le processeur 12 qui n'ont aucune utilité fonctionnelle pour le processeur. Par exemple, un tel message sans aucune utilité fonctionnelle peut être :

- un message de consultation de données inexistantes dans le processeur,
- un message d'effacement d'une donnée inexistante (par exemple : code d'accès, ...) dans le processeur, ou
- deux messages successifs de lecture de la même donnée du processeur 12.

[0040] Ces messages sont syntaxiquement correctes et ne provoquent aucune erreur d'exécution dans le processeur 12. Par contre ils sont inutiles. De tels messages inutiles peuvent être envoyés, par erreur, par l'opérateur. Ils peuvent également être utilisés lors d'une tentative d'attaque.

[0041] Le compteur C_4 dénombre le nombre d'erreurs de syntaxe dans les messages transmis au processeur 12 c'est-à-dire typiquement dans les messages ECM et EMM transmis à ce processeur. En effet, la syntaxe ou structure des messages ECM et EMM respecte une grammaire prédéterminée. Le processeur 12 peut donc détecter ces erreurs de syntaxe et les comptabiliser dans le compteur C_4. Les erreurs de syntaxes peuvent être provoquées par une erreur de l'opérateur mais également lors d'une tentative d'attaque.

[0042] Le compteur C_5 est un compteur de commandes rejouées alors qu'elles ne devraient normalement pas être rejouées plusieurs fois. Le rejeu d'une commande consiste à envoyer au processeur de sécurité plusieurs fois la même commande. Par exemple, la commande peut être un message de mise à jour de certaines données enregistrées dans le processeur 12. Un rejeu d'un message peut être détecté par le processeur 12 en enregistrant la date du dernier message de mise à jour.

[0043] Le compteur C_6 dénombre le nombre d'erreurs d'intégrité détectées dans les messages reçus par le processeur 12. En effet, les messages reçus par le processeur 12, contiennent des données ainsi qu'une redondance cryptographique de ces données, ce qui permet au processeur 12 de vérifier qu'il n'y a pas d'erreur dans les données reçues. Par exemple, la redondance sur les données peut être obtenue en intégrant dans le message reçu une signature ou un CRC (« Cyclic Redondancy Check ») des données contenues dans ce message. Des erreurs dans les données contenues dans le message peuvent être provoquées par des perturbations lors de leur transport dans le réseau 8 ou dans le décodeur 10. Toutefois, des données erronées sont aussi utilisées lors d'une tentative d'attaque.

[0044] Le compteur C_7 dénombre le nombre d'erreurs d'intégrité sur des données contenues dans le processeur 12. En effet, un certain nombre de données enregistrées dans le processeur 12 sont associées à une redondance cryptographique permettant de vérifier l'intégrité de la donnée enregistrée respective.

Encore une fois, il peut arriver accidentellement, suite par exemple à des perturbations électromagnétiques, qu'une donnée enregistrée dans le processeur 12 soit erronée. Toutefois, la présence de données erronées enregistrées dans le processeur 12 peut également être représentative d'une tentative d'attaque.

[0045] Le compteur C_8 dénombre le nombre de déroutements lors l'exécution du code du système d'exploitation du processeur 12. Un déroutement est un saut intempestif ou erroné d'une instruction du code exécuté par le processeur 12 vers une autre instruction. Ces déroutements dans l'exécution du code peuvent être détectés en exécutant deux fois de suite les mêmes instructions sur les mêmes données. Si les deux exécutions du code ne donnent pas le même résultat, cela signale un déroutement. Des sauts intempestifs d'instructions dans le code exécuté par le processeur 12 peuvent être provoqués en jouant sur la tension d'alimentation du processeur 12 ou en dirigeant un faisceau laser vers ce processeur 12.

[0046] Le compteur C_9 dénombre le nombre de fois où la procédure de récupération de données suite à un arrachement du processeur 12 est exécutée. L'arrachement du processeur 12 consiste à retirer, en cours de fonctionnement, le processeur 12 du décodeur 10 de sorte que l'alimentation du processeur 12 est interrompue en cours de traitement de données. La procédure de récupération de données permet de remettre, après une telle coupure d'alimentation, le processeur 12 dans l'état dans lequel il était avant cette coupure d'alimentation. Le processeur 12 peut être arraché accidentellement du décodeur 10. Toutefois, des coupures intempestives de l'alimentation du processeur 12 sont également fréquemment utilisées lors d'une tentative d'attaque pour empêcher l'exécution par le processeur 12 de contre-mesures.

[0047] Le compteur C_{10} dénombre le nombre de fois où une tension d'alimentation anormale est mesurée par le capteur 26 cumulé au nombre de fois où un faisceau laser est détecté par le capteur 27. En effet, des tensions anormales ainsi que la présence d'un faisceau laser sont typiques d'une tentative d'attaque du processeur 12. Toutefois, ces capteurs 26 et 27 peuvent également détecter une tension anormale ou la présence d'un faisceau laser accidentellement suite, par exemple, à des perturbations électromagnétiques causées par un appareil à proximité du processeur 12 et cela même en absence de tentative d'attaque. Par exemple, la mise sous tension du décodeur 12 peut se traduire par la détection d'une tension anormale par le capteur 26.

[0048] Le compteur C_0 est à distinguer des compteurs précédents puisque celui-ci dénombre un événement qui se produit uniquement lors du fonctionnement normal du processeur 12 et qui ne peut pas être provoqué par une tentative d'attaque. Par exemple, l'événement dénombré par le compteur C_0 est ici le nombre de messages ECM et EMM correctement traités par le processeur 12.

[0049] La valeur de ce compteur C_0 est utilisée pour limiter la mémoire temporelle de certains des compteurs précédents à une fenêtre temporelle glissante de durée finie. Par exemple, à cet effet, la valeur du compteur C_0 est soustraite à la valeur du compteur C_i, où $i > 0$, et seule la différence entre ces deux compteurs, ramenée à zéro si elle est négative, est utilisée dans le calcul d'un indice de concomitance comme décrit plus loin. Par exemple, ici, à l'exception de la valeur des compteurs C_8 et C_{10}, seule la différence entre les valeurs des compteurs C_i et C_0 est utilisée pour le calcul des indices de concomitance. Grâce à l'utilisation de la valeur du compteur C_0, les événements qui se sont produits en dehors de la fenêtre temporelle glissante ainsi définie ne sont pas pris en compte pour la détection d'une tentative d'attaque. On notera que la durée de la fenêtre temporelle glissante définie à l'aide du compteur C_0 n'est pas constante et dépend de l'utilisation qui est faite du processeur 12.

[0050] Le calculateur 24 est raccordé à une mémoire 32 contenant les différentes données et instructions nécessaires au fonctionnement du processeur 12. En particulier, la mémoire 32 comprend :

- les instructions nécessaires à l'exécution du procédé de la figure 4 lorsqu'elles sont exécutées par le calculateur 24,
- une matrice 36 de coefficients de pondération et une table 38 de seuils d'alerte.

[0051] Un exemple de matrice 36 est représenté plus en détail dans figure 2. Cette matrice 36 contient autant de colonnes que de compteurs d'événement susceptible d'être déclenché par une tentative d'attaque. Ici, la matrice 36 est donc une matrice à dix colonnes associées chacune à un compteur C_i. La matrice 36 contient également neuf lignes associées, respectivement, aux compteurs C_2 à C_{10}.

[0052] La cellule située au croisement de la i-ème colonne en partant de la gauche et de la j-ième ligne en partant du haut contient un coefficient $m_{i,j}$ de pondération associé à un indice de concomitance C_iC_{j+1}. Un indice de concomitance C_iC_{j+1} est un indice calculé à partir de la valeur des compteurs C_i et C_{j+1} qui fournit une indication sur la concomitance entre les événements dénombrés par le compteur C_i et ceux dénombrés par le compteur C_{j+1}. Ici, chaque indice de concomitance est construit de manière à ce que sa valeur soit d'autant plus élevée qu'un grand nombre d'événements mesurés, respectivement, par les compteurs C_i et C_{j+1} s'est produit à proximité du même instant. A cet effet, dans ce mode de réalisation, chaque indice de concomitance C_iC_{j+1} correspond au produit des valeurs des compteurs C_i et C_{j+1} au même instant.

[0053] La table 38 de seuils d'alerte illustrée sur la figure 3 comprend une première colonne contenant quatre seuils d'alerte S_1 à S_4. Chaque seuil d'alerte est une valeur numérique et ces seuils d'alerte sont classés par ordre croissant en allant du haut vers le bas dans la table 38.

[0054] La table 38 contient également une deuxième colonne associant à chaque seuil S_i une ou plusieurs contre-mesures notées CM_i. Les contre-mesures sont des actions exécutées par le processeur de sécurité 12 qui visent à rendre plus difficile l'extraction ou la détermination de données contenues dans le processeur 12 ou l'utilisation abusive de ce processeur 12.

[0055] Ici, les contre-mesures CM_i associées au seuil S_i sont moins sévères et moins invalidantes pour l'utilisateur du processeur que celles associées au seuil d'alerte supérieur S_{i+1}. Ainsi, plus le seuil d'alerte S_i franchi est élevé plus les contre-mesures CM_i exécutées en réponse sont sévères.

[0056] A titre d'illustration, les contre-mesures CM_1 consistent à ajouter de la redondance sur les branchements conditionnels du code à exécuter par le processeur 12. Par exemple, cette redondance est obtenue en exécutant plusieurs fois le branchement conditionnel et en vérifiant qu'à chaque exécution le résultat obtenu est le même.

[0057] La contre-mesure CM_1 consiste à ajouter en plus de la redondance sur les opérations de vérification de l'intégrité des données traitées. Par exemple, l'intégrité des données est vérifiée plusieurs fois alors que si le seuil S_1 n'est pas franchi, elle n'est vérifiée qu'une fois. Cela consiste également à vérifier l'intégrité de données dont l'intégrité n'est pas vérifiée si le seuil S_1 n'est pas franchi.

[0058] Les contre-mesures CM_2 consistent, par exemple, à ajouter des restrictions sur les possibilités de chaîner des instructions du code exécuté par le processeur 12. Ceci peut être obtenu en obligeant le processeur 12 à exécuter un bloc complet d'instructions sans permettre d'interruption entre l'exécution des instructions de ce bloc.

[0059] La contre-mesure CM_2 consiste également à supprimer certaines fonctionnalités du processeur 12 auparavant autorisées lorsque le seuil S_2 n'était pas franchi. Par exemple, l'ajout de nouveaux services tel que l'ajout d'un nouvel opérateur ou d'un nouvel abonnement est interdit. L'accès aux fonctionnalités d'administration du processeur 12 peut également être interdit si le seuil S_2 est franchi.

[0060] Par exemple, les contre-mesures CM_3 consistent à modifier les coefficients de pondération présents dans la matrice 36 de manière à ce que le seuil supérieur c'est-à-dire S_4, soit facilement et rapidement atteint lorsque des événements sont mesurés. Ainsi, comme cela est décrit en regard de la figure 4, on augmente la sensibilité du processeur 12 à la détection d'une tentative d'attaque. Les contre-mesures CM_3 comprennent également la vérification systématique et en double de l'intégrité de chaque message reçu. Les contre-mesures CM_3 peuvent également consister à renforcer les contrôles du flux d'exécution. Cela peut notamment consister à exécuter deux fois chaque portion du code exécutable par le processeur 12 et à

comparer à l'issue de ces deux exécutions que les résultats obtenus sont les mêmes. En cas de discordance entre les résultats obtenus, le compteur C_8 est incrémenté.

[0061] Enfin, les contre-mesures CM_4 consistent à invalider de façon définitive le processeur 12 de manière à ce que celui-ci soit définitivement inutilisable. Par exemple, à cet effet, les informations confidentielles contenues dans le processeur 12 sont effacées.

[0062] Le fonctionnement du processeur 12 va maintenant être décrit plus en détail en regard du procédé de la figure 4.

[0063] En parallèle du fonctionnement normal du processeur 12, celui-ci exécute également un procédé de détection d'une tentative d'attaque. A cet effet, lors d'une étape 50, il mesure les événements susceptibles d'être causés par une tentative d'attaque. Ici, cette mesure consiste à comptabiliser dans les compteurs C_i l'événement correspondant.

[0064] Ensuite, lors d'une étape 52, le processeur 12 construit trois indicateurs d'attaque, respectivement, I_1, I_2 et I_3.

[0065] L'indicateur I_1 est conçu pour être plus sensible aux tentatives d'attaque par perturbation laser que les indicateurs I_2 et I_3. Une attaque par perturbation laser consiste à diriger un faisceau laser sur le processeur de sécurité pour provoquer des sauts d'instructions dans le code exécuté par ce processeur à des moments clé de son exécution. Les moments clés correspondent typiquement à des branchements conditionnels.

[0066] Ici, la valeur de l'indicateur I_1 est donnée par la relation suivante :

$$I_1 = m_{2,6}C_2C_7 + m_{2,7}C_2C_8 + m_{2,9}C_2C_{10} + m_{7,7}C_7C_8 + m_{7,9}C_7C_{10} + m_{8,9}C_8C_{10}$$

où :

- $m_{i,j}$ est le coefficient de pondération dont la valeur est contenue dans la matrice 36.

[0067] L'indicateur I_2 est conçu pour être plus sensible que les deux autres aux attaques logiques. Une attaque logique consiste à rechercher une faille logicielle ou une erreur d'implémentation dans le code exécuté par le processeur 12 de manière à obtenir un comportement anormal de ce processeur. Par exemple, l'attaque logique consiste à envoyer un très grand nombre de messages erronés au processeur 12 tous différents les uns des autres jusqu'à ce que l'un de ces messages provoque un comportement anormal du processeur 12.

[0068] Par exemple, la valeur de l'indicateur I_2 est construite à l'aide de la relation suivante :

$$I_2 = m_{1,2}C_1C_3 + m_{1,3}C_1C_4 + m_{3,3}C_3C_4$$

[0069] Enfin, l'indicateur I_3 est conçu pour être plus sensible aux tentatives d'attaque DPA (Differential Power Analysis). Une attaque DPA consiste à envoyer un grand nombre de messages au processeur 12 pour provoquer un grand nombre d'exécutions des algorithmes cryptographiques sur un grand nombre de données

différentes et à mesurer, en parallèle, la consommation de courant du processeur 12. Ensuite, par une analyse statistique sur les données recueillies, il est possible de découvrir quelles sont les valeurs des clefs ou des données confidentielles enregistrées dans le processeur 12.

[0070] Par exemple, l'indicateur I_3 est construit à l'aide de la relation suivante :

$$I_3 = m_{4,4}C_4C_5 + m_{4,5}C_4C_6 + m_{5,5}C_5C_6.$$

[0071] Ensuite, une fois que la valeur des indicateurs I_1 à I_3 a été construite, lors d'une étape 54, la valeur de ces indicateurs est comparée aux différents seuils d'alerte enregistrés dans la table 38 pour détecter une tentative d'attaque.

[0072] Si la valeur d'aucun de ces indicateurs ne franchit le seuil S_1, alors, lors d'une étape 56, aucune contre-mesure n'est exécutée.

[0073] A l'inverse, si la valeur d'un de ces indicateurs franchit l'un des seuils S_i, alors les contre-mesures associées au seuil S_i le plus élevé franchi sont exécutées lors d'une étape 58.

[0074] A l'issue des étapes 56 et 58, le procédé retourne à l'étape 50.

[0075] En parallèle des étapes 50 à 58, lors d'une étape 60, l'émetteur 4 transmet, par exemple par l'intermédiaire d'un message EMM ou ECM, de nouvelles valeurs pour les coefficients de pondération. Ensuite, lors d'une étape 62, le processeur 12 reçoit ce message et met à jour les valeurs des coefficients de pondération contenus dans la matrice 36.

[0076] La mise à jour des coefficients de pondération permet de modifier facilement la sensibilité d'un indicateur à une tentative d'attaque particulière. En particulier, on remarquera que pour modifier cette sensibilité de l'indicateur à une tentative d'attaque particulière, il est uniquement nécessaire de modifier les coefficients de pondération enregistrés dans la matrice 36 sans qu'il soit nécessaire de modifier d'autres instructions exécutables par le processeur 12.

[0077] De nombreux autres modes de réalisation sont possibles. Par exemple, le processeur 12 peut comporter plusieurs matrices différentes de coefficients de pondération. Chacune de ces matrices peut être utilisée pour calculer un indicateur d'attaque respectif. Cela permet alors d'affecter à chaque indice de concomitance un coefficient de pondération différent en fonction de l'indicateur d'attaque construit. L'utilisation de plusieurs matrices de coefficients de pondération peut être aussi utile pour modifier la matrice de pondération utilisée lorsqu'un nouveau seuil d'alerte est franchi.

[0078] A l'inverse, un seul indicateur d'attaque peut être construit au lieu de plusieurs.

[0079] En variante, il existe autant de tables de seuils d'alerte que d'indicateurs d'attaque construits. Dans cette variante, les seuils d'alerte associés à un indicateur d'attaque particulier ne sont donc pas nécessairement les mêmes que les seuils d'alerte associés à un autre indicateur d'attaque.

[0080] La table 38 peut également être remplacée par un seul seuil d'alerte associé à des contre-mesures.

[0081] L'un des compteurs C_i peut simplement comptabiliser l'existence d'un événement sans comptabiliser le nombre d'occurrences de cet événement. Dans ce cas, la valeur de ce compteur est codable à l'aide d'un seul bit d'information. Même dans ce cas, la valeur de ce compteur d'existence peut être associé à une fenêtre temporelle de durée infinie ou finie.

[0082] D'autres capteurs que ceux décrits peuvent être implémentés dans le processeur 12. Par exemple, le processeur 12 peut également comporter un capteur de température.

[0083] L'indice de concomitance n'est pas limité au produit de deux mesures. Par exemple, il peut aussi correspondre à un produit de plus de deux mesures. Toutefois, l'augmentation du nombre de mesures multipliées entre elles augmente également la taille de la matrice de coefficients de pondération.

[0084] Il est également possible de calculer un indice de concomitance représentant la proximité temporelle entre au moins deux événements par d'autres opérations mathématiques qu'un produit.

[0085] De nombreuses autres contre-mesures que celles précédemment indiquées peuvent être exécutées en réponse au franchissement d'un seuil d'alerte par l'un des indicateurs d'attaque. Par exemple, d'autres contre-mesures peuvent consister à modifier l'algorithme cryptographique exécuté par le processeur 12. Une contre-mesure peut également consister à utiliser ou à mesurer de nouveaux événements pour construire un indicateur d'attaque qui auparavant n'était pas mesuré. Par exemple, en réponse au franchissement d'un seuil d'alerte, les événements mesurés par l'un des capteurs 26 ou 27 peuvent être comptabilisés alors qu'auparavant ils ne l'étaient pas.

[0086] Le calculateur 24 peut être formé d'un seul ou de plusieurs processeurs. Par exemple, il peut être formé d'un processeur auquel est associé un coprocesseur. Le procédé de détection peut alors être exécuté aussi bien par le processeur que par le co-processeur.

[0087] La mesure a été ici décrite dans le cas particulier où il s'agit de comptabiliser le nombre d'occurrences d'un événement. Toutefois, la mesure peut également consister à enregistrer dans l'un des registres la valeur d'un événement tel que par exemple une valeur mesurée par l'un des capteurs 26 ou 27. Pour compter le nombre d'occurrences d'un événement, la valeur des compteurs peut également être décrémentée au lieu d'être incrémentée comme décrit précédemment.

[0088] L'architecture du récepteur 6 est ici uniquement illustrative d'une situation particulière. En particulier, le désembrouilleur 18 peut également être amovible. A l'inverse, le désembrouilleur et le processeur de sécurité peuvent être implémentés

sans aucun degré de liberté dans le décodeur. Dans ce cas, le désembrouilleur et le processeur de sécurité peuvent se présenter sous la forme de composant logiciel.

REVENDICATIONS

1. Procédé de détection d'une tentative d'attaque d'un processeur de sécurité par le processeur de sécurité lui-même, ce procédé comprenant des mesures (50) de plusieurs événements différents se produisant indépendamment les uns des autres en absence de tentative d'attaque,
caractérisé en ce que le procédé comprend également :
- la construction (52) de la valeur d'au moins un indicateur d'attaque en fonction d'au moins un indice de concomitance entre au moins deux événements différents mesurés, l'indice de concomitance étant représentatif de la proximité temporelle entre les deux événements différents mesurés, et
- la détection (54) d'une tentative d'attaque si la valeur de l'indicateur d'attaque franchit un seuil prédéterminé.

2. Procédé selon la revendication 1, dans lequel la valeur de l'indicateur d'attaque est construite (52) à partir de plusieurs indices de concomitance entre des événements différents mesurés et en pondérant l'importance de ces indices de concomitance les uns par rapport aux autres à l'aide d'un jeu prédéterminé de coefficients de pondération.

3. Procédé selon la revendication 2, dans lequel le procédé comprend la construction (52) de plusieurs valeurs d'indicateurs d'attaque en utilisant plusieurs jeux différents de coefficients de pondération entre les mêmes indices de concomitance, chaque jeu de coefficients de pondération étant prédéterminé pour être plus sensible à une tentative d'attaque différente de celles auxquelles sont plus sensibles les autres indicateurs.

4. Procédé selon la revendication 3, dans lequel le coefficient de pondération d'un même indice de concomitance est le même dans tous les jeux de coefficients de pondération utilisés pour construire les différentes valeurs d'indicateurs d'attaque.

5. Procédé selon l'une quelconque des revendications précédentes, dans lequel la mesure (50) d'un événement est limitée à une fenêtre temporelle glissante de manière à ne pas prendre en compte des événements qui se sont produits en dehors de cette fenêtre temporelle.

6. Procédé selon l'une quelconque des revendications précédentes, dans lequel au moins l'un des événements mesurés est la détection d'une erreur de fonctionnement

du processeur de sécurité dont chaque occurrence conduit le processeur de sécurité à arrêter les traitements en cours et à se réinitialiser automatiquement pour reprendre ces traitements depuis le début.

7. Procédé selon l'une quelconque des revendications précédentes, dans lequel la mesure (50) d'un événement consiste à comptabiliser dans un compteur le nombre de fois où cet événement s'est produit, la valeur du compteur constituant la mesure.

8. Procédé selon l'une quelconque des revendications précédentes, dans lequel l'indice de concomitance entre au moins deux mesures est obtenu en multipliant entre elles ces mesures.

9. Support d'enregistrement d'informations, caractérisé en ce qu'il comporte des instructions pour l'exécution d'un procédé de détection conforme à l'une quelconque des revendications précédentes, lorsque ces instructions sont exécutées par un calculateur électronique.

10. Processeur de sécurité comportant :
- des registres (C_1 à C_{10}) dans lesquels sont stockées des mesures de plusieurs événements se produisant indépendamment les uns des autres en absence de tentative d'attaque, et
- un calculateur (24),

caractérisé en ce que le calculateur (24) est apte :
- à construire la valeur d'au moins un indicateur d'attaque en fonction d'au moins un indice de concomitance entre au moins deux événements différents mesurés dont les mesures sont stockées dans les registres, cet indice de concomitance étant représentatif de la proximité temporelle entre les deux événements différents mesurés, et
- à détecter une tentative d'attaque si la valeur de l'indicateur d'attaque franchit un seuil prédéterminé.

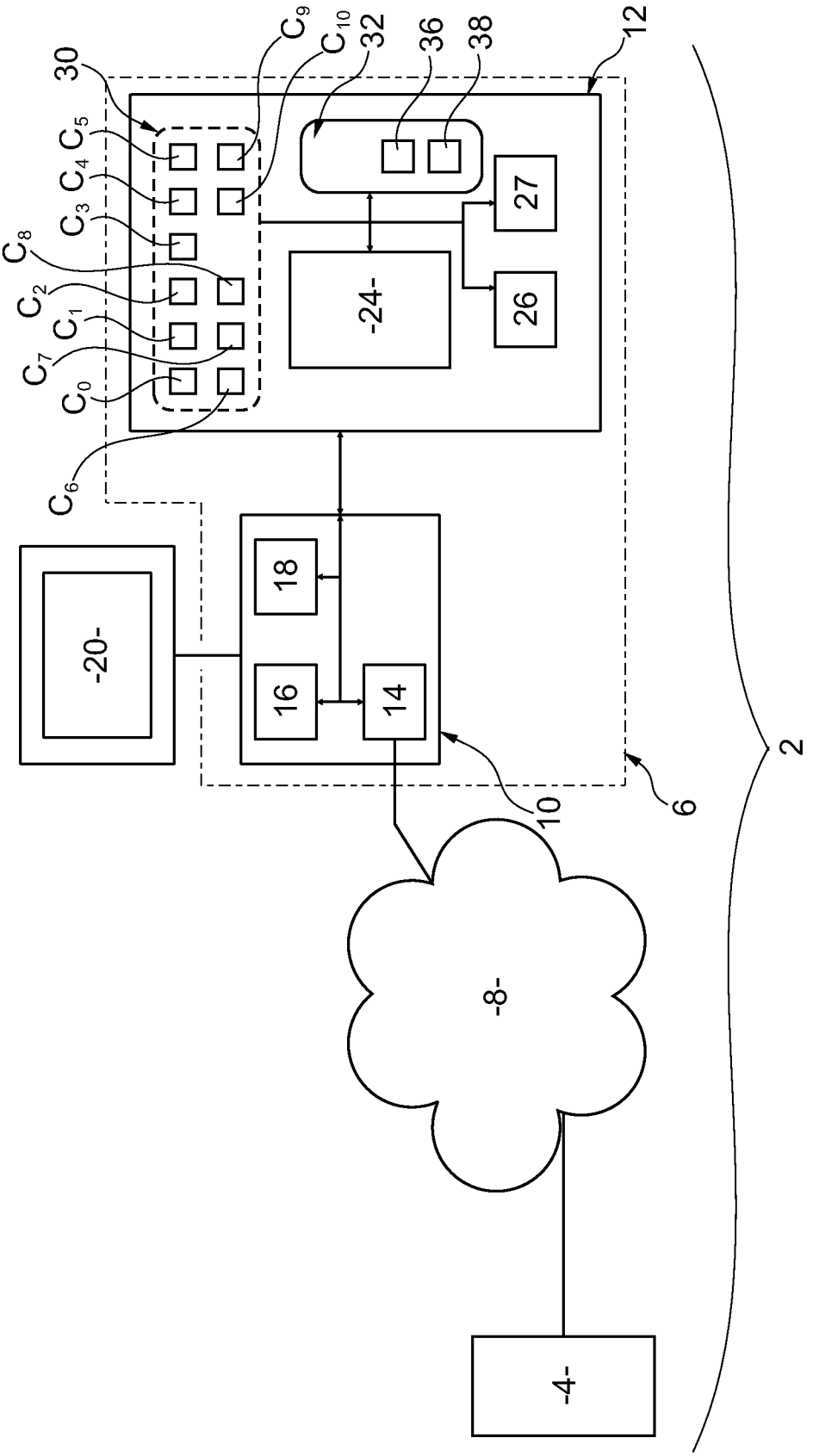
30
C5
C4
C3
C8
C2
C1
C7
C0
C6
C9
C10
32
36
38
12
27
26
-24-
18
16
14
-20-
10
6
2
-8-
-4-

Fig. 1

	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10
C2		0	0	0	0	0	0	0	0	0
C3	100		0	0	0	0	0	0	0	0
C4	100		50	0	0	0	0	0	0	0
C5				1	0	0	0	0	0	0
C6					1	0	0	0	0	0
C7		20000					0	0	0	0
C8		20000					10000	0	0	0
C9									0	0
C10		4000					2000	2000		0

36

Fig. 2

S_1	CM_1
S_2	CM_2
S_3	CM_3
S_4	CM_4

38

Fig. 3

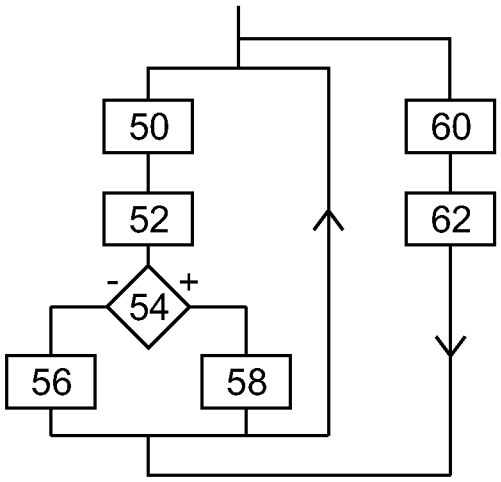

Fig. 4

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2010/058949

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00
ADD. G06F21/02

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 533 123 A (FORCE GORDON [US] ET AL) 2 July 1996 (1996-07-02) column 1, line 5 - line 30 column 2, line 37 - line 39 column 22, line 12 - line 23 column 23, line 16 - column 25, line 12 column 30, line 56 - column 31, line 19	1-10

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
5 October 2010	08/11/2010

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Fax: (+31–70) 340–3016	Arbutina, Ljiljana

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2010/058949

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5533123 A	02-07-1996	DE 69519662 D1	25-01-2001
		DE 69519662 T2	23-05-2001
		EP 0715733 A1	12-06-1996
		WO 9600953 A2	11-01-1996

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/EP2010/058949

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. G06F21/00
ADD. G06F21/02

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	US 5 533 123 A (FORCE GORDON [US] ET AL) 2 juillet 1996 (1996-07-02) colonne 1, ligne 5 - ligne 30 colonne 2, ligne 37 - ligne 39 colonne 22, ligne 12 - ligne 23 colonne 23, ligne 16 - colonne 25, ligne 12 colonne 30, ligne 56 - colonne 31, ligne 19 -----	1-10

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
5 octobre 2010	08/11/2010

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Fax: (+31–70) 340–3016	Arbutina, Ljiljana

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/EP2010/058949

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 5533123 A	02-07-1996	DE 69519662 D1	25-01-2001
		DE 69519662 T2	23-05-2001
		EP 0715733 A1	12-06-1996
		WO 9600953 A2	11-01-1996