EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention of the grant of the patent:
15.12.2010 Bulletin 2010/50

(21) Application number: 02765244.5

(22) Date of filing: 12.09.2002

(54) CALCULATION OF IDENTIFIER CODES

BERECHNUNG VON KENNUNGSCODES
CALCUL DE CODES D'IDENTIFICATEUR

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LU MC NL PT SE SK TR


(43) Date of publication of application:
23.06.2004 Bulletin 2004/26

(73) Proprietor: NXP B.V.
5656 AG Eindhoven (NL)

(72) Inventors:
• PISARSKY, Vladimir, R.
  NL-5656 AA Eindhoven (NL)

• SHTEYN, Yevgeniy, E.
  NL-5656 AA Eindhoven (NL)

(74) Representative: Williamson, Paul Lewis et al
NXP Semiconductors UK Ltd.
Intellectual Property Department
Betchworth House
57-65 Station Road
Redhill
Surrey RH1 1DL (GB)

(56) References cited:
US-A-6 067 621

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).
Description

FIELD OF THE INVENTION

[0001] The invention relates to a method of providing an authentication service, e.g., for secure transactions with a data processing system.

BACKGROUND ART

[0002] The non-prepublished application PCT/IB02/01582 (attorney docket PHUS 018056) for DEVICE IDENTIFICATION AND CONTROL IN NETWORK ENVIRONMENT relates to a control network for home appliances comprising a module for interfacing an appliance to the network. The module adopts the identity of the appliance when the module and the appliance are being interconnected. The appliance comprises a tag, e.g., in its power plug, with identifying information that gets read by the module and transferred to a controller. The module itself can have a location dependent identifier to enable topology dependent software applications.

[0003] The non-prepublished application PCT/IB02/01015 (attorney docket PHUS 018043) for TASK MANAGEMENT SYSTEM relates to a system for managing tasks involving the movement of an object. The system includes an indicator attached to the object, and a sensor for detecting the position or movement of the object, for use with a monitoring component, e.g., for generating and canceling in a user-interface reminders to perform the task based upon input from the sensor. In one embodiment, the indicator is, e.g., a radio frequency, passive device connected to the object, the sensor is a conventional proximity sensor positioned within the path of travel the object will follow when the task is performed, and the monitoring component is part of a home network linked to a PDA (Personal Digital Assistant). In another embodiment, two or more sensors are used to establish the position of the object at a first location (start location) and the position of the object at a second location (destination) and/or direction of movement of the object, rather than merely detect movement of the object past a location within the path of travel. In both embodiments, the sensors detect presence/absence of the object at predetermined locations and/or movement of the object (by sensing the indicator) when the task is being performed, and provide a signal to the monitoring component indicating that the task is being completed. The monitoring component then generates a response such as automatically removing the reminder to perform the task.

[0004] Identifier data, passwords or code words, referred to as ID in the remainder of this text, are being used for security purposes in electronic transactions wherein identification or authentication of the user is required. Examples of such transactions include those based on the use of credit cards. Another example is electronic banking. Yet another example is logging in into a company’s data network from a remote location and via the Internet. Yet another usage is badge access to secure sites.

[0005] In general, the following scheme is implemented. The user has been assigned an ID. The ID has to be memorized or is encrypted on some token, e.g., a card with a magnetic strip or solid state memory, a CE device such as a cellphone, etc. In order to perform an operation or transaction involving this ID, it is required for the user to transmit the ID to a controlling computer (e.g., a bank computer, the computer of a telecom service provider, a security server, etc.). The computer then compares the transmitted ID with the code stored locally in order to make an authorization decision based on the match or mismatch.

[0006] There are some drawbacks involved in this practice. For example, the ID is usually constant (i.e., does not change with time) and can be intercepted during transmission, or the token that contains the ID can be stolen. The first disadvantage can be avoided by the use of onetime encrypt codes: a new value for the ID is calculated each time a new connection with a server is required. However, this solves only part of the security problem as it is still possible to crack the code or get the information from an independent source. After some time period of data collection it may be well possible to reverse engineer the required codes. The one-time encrypt code does not solve the problem of the token being lost or stolen.

[0007] US 5,590,199 discloses a system for authenticating and authorizing a user to access services on a heterogeneous computer network. The system includes at least one workstation and one authorization server connected to each other through a network. A user couples a personally protectable coprocessor (smart card) to the workstation by means of a bidirectional communications channel.

SUMMARY OF THE INVENTION

[0008] In a first aspect, the present invention provides a method of determining an ID value for a user, as claimed in claim 1.

[0009] In a further aspect the present invention provides a personal appliance for use in a personal network, as claimed in claim 3.

[0010] In one embodiment, the inventors propose to increase security level by means of distributing the calculation of a new value of the ID between the user’s personal electronic devices. The server or computer that decides on authorization has a simulation running per individual user of the same personal devices to synchronize the ID’s values. In this case, it is not enough to steal just one ID code card or credit card. Without the other devices or the user, the card is useless.

[0011] The invention relates to a method of enabling a person to use a unique ID. Multiple devices of a PAN (Personal Area Network) of the user are used to calculate the ID in a manner distributed among the devices. The
system that has to determine whether or not the user’s ID is proper can do that by checking if the ID is in conformity with a simulation of the PAN run on a remote server. Alternatively, the various IDs generated by the PAN on different occasions each are representative of this particular user and correspond to an entry in a look-up table. Preferably, each respective one of the devices comprises a respective FSM (Finite State Machine). The respective FSM calculates per time step a value of a quantity according to a respective mathematical relationship. The respective mathematical relationship has as arguments, e.g., the value of the quantity calculated at a preceding time step by at least another one of the FSMS; and a respective history of values assumed by the quantity calculated by the respective FSM. The respective mathematical relationship is such that the quantity assumes a practically stochastic behavior.

Another embodiment is, e.g., a personal appliance for use in the PAN. The appliance accommodates an FSM and is capable of communicating with another appliance in the PAN for implementing the practically stochastic system.

Yet another embodiment is a service for, e.g., a banking-, credit card-, conditional access- or another security system. The service determines whether a user is authorized to access the system. The service runs a simulation of a PAN of the user. This service could be delegated to a trusted party independent of the system to be secured, or could be an integral part of the system.

In a more specific example, the invention considers a distributed information processing system that comprises a cluster of interacting devices or appliances forming, e.g., a personal area network (PAN). The devices communicate preferably through a short-range, wireless protocol, e.g., Bluetooth. The cluster comprises, for example, a cellphone, a digital watch, a PDA, the key fob of the car keys, an electronic device embedded in an inconspicuous object such as a piece of jewelry or a pin, or even in a piece of clothing using wearable electronics, etc., etc. The set of devices is unique per individual user. The devices have finite state machines (FSMs) onboard. A (remote) control server runs a simulator of the cluster’s FSMs. Each respective device’s FSM calculates per time step a respective numerical value that depends on the values of the other devices’ FSMS in the previous step, possibly also on the respective device’s internal state (e.g., based on the device’s memory’s and I/O message buffers’ content), and on a history of the previous values. This mathematical relationship is chosen such that it causes the collection of FSMS to behave as a dynamic process that is considered, for practical purposes, a non-periodic stochastic process. The simulator does the same on the server. The results of the simulator and the devices’ FSMS should be identical. Upon a match, the user is assumed to be authorized. Upon a mismatch, the user is assumed to be non-authorized, and an alert can be generated. The ID’s value is, e.g., the current numerical value calculated by a specific one of the FSMS, or a combination of values from different FSMS, or a sequence of values, etc.

The security of the system resides in the facts that in order to be able to hack the system, the hacker needs to have a snapshot of the values of all FSM at a certain step, to collect the values of the steps taken into account in the history, and to get into the internal states of each device. All these manipulations need to be performed in one time step, which makes it a complex computational task and practically impossible due to the distributed character of the system. Several security layers that can be applied individually or combined in order to increase protection, robustness and security of the system.

In a more specific example, the invention considers a distributed information processing system that comprises a cluster of interacting devices or appliances forming, e.g., a personal area network (PAN). The devices communicate preferably through a short-range, wireless protocol, e.g., Bluetooth. The cluster comprises, for example, a cellphone, a digital watch, a PDA, the key fob of the car keys, an electronic device embedded in an inconspicuous object such as a piece of jewelry or a pin, or even in a piece of clothing using wearable electronics, etc., etc. The set of devices is unique per individual user. The devices have finite state machines (FSMs) onboard. A (remote) control server runs a simulator of the cluster’s FSMs. Each respective device’s FSM calculates per time step a respective numerical value that depends on the values of the other devices’ FSMS in the previous step, possibly also on the respective device’s internal state (e.g., based on the device’s memory’s and I/O message buffers’ content), and on a history of the previous values. This mathematical relationship is chosen such that it causes the collection of FSMS to behave as a dynamic process that is considered, for practical purposes, a non-periodic stochastic process. The simulator does the same on the server. The results of the simulator and the devices’ FSMS should be identical. Upon a match, the user is assumed to be authorized. Upon a mismatch, the user is assumed to be non-authorized, and an alert can be generated. The ID’s value is, e.g., the current numerical value calculated by a specific one of the FSMS, or a combination of values from different FSMS, or a sequence of values, etc.

The security of the system resides in the facts that in order to be able to hack the system, the hacker needs to have a snapshot of the values of all FSM at a certain step, to collect the values of the steps taken into account in the history, and to get into the internal states of each device. All these manipulations need to be performed in one time step, which makes it a complex computational task and practically impossible due to the distributed character of the system. Several security layers that can be applied individually or combined in order to increase protection, robustness and security of the system.

In a more specific example, the invention considers a distributed information processing system that comprises a cluster of interacting devices or appliances forming, e.g., a personal area network (PAN). The devices communicate preferably through a short-range, wireless protocol, e.g., Bluetooth. The cluster comprises, for example, a cellphone, a digital watch, a PDA, the key fob of the car keys, an electronic device embedded in an inconspicuous object such as a piece of jewelry or a pin, or even in a piece of clothing using wearable electronics, etc., etc. The set of devices is unique per individual user. The devices have finite state machines (FSMs) onboard. A (remote) control server runs a simulator of the cluster’s FSMs. Each respective device’s FSM calculates per time step a respective numerical value that depends on the values of the other devices’ FSMS in the previous step, possibly also on the respective device’s internal state (e.g., based on the device’s memory’s and I/O message buffers’ content), and on a history of the previous values. This mathematical relationship is chosen such that it causes the collection of FSMS to behave as a dynamic process that is considered, for practical purposes, a non-periodic stochastic process. The simulator does the same on the server. The results of the simulator and the devices’ FSMS should be identical. Upon a match, the user is assumed to be authorized. Upon a mismatch, the user is assumed to be non-authorized, and an alert can be generated. The ID’s value is, e.g., the current numerical value calculated by a specific one of the FSMS, or a combination of values from different FSMS, or a sequence of values, etc.

The security of the system resides in the facts that in order to be able to hack the system, the hacker needs to have a snapshot of the values of all FSM at a certain step, to collect the values of the steps taken into account in the history, and to get into the internal states of each device. All these manipulations need to be performed in one time step, which makes it a complex computational task and practically impossible due to the distributed character of the system. Several security layers that can be applied individually or combined in order to increase protection, robustness and security of the system.

The invention is further explained below, by way of example and with reference to the accompanying drawing, showing a diagram of a system in the invention.

In the detailed discussion below the following definitions are being used:

- **SYSTEM**: the conglomeration of the devices under consideration in the PAN;
- **DEVICE**: a component of the SYSTEM that includes a CPU-based controller;
- **DEVICE STATE INFORMATION (DSI)**: control code calculated by some rules in the DEVICE’s memory, possibly including the DEVICE’s I/O message buffers;
- **CONTROL SERVER**: computer outside the SYSTEM that is monitoring operations of the SYSTEM;
- **SIMULATOR**: simulation software simulating the SYSTEM as a distributed network of FSMS.

The drawing is a block diagram of a system 100 in the invention. System 100 comprises a SYSTEM 102, e.g., a PAN. SYSTEM 102 includes DEVICES
104, 106, ..., 108. Each of DEVICES 104-108 has a respective FSM 110, 112, ..., 114. System 100 further comprises a CONTROL SERVER 116 that runs a SIMULATOR 118 simulating the behavior of SYSTEM 102 in software. The results of SIMULATOR 118 are compared with the states of DEVICES 104-108 in an evaluator 120 to determine whether or not the user is authorized.

[0021] In a first one of the security layers SIMULATOR 118 is run on CONTROL SERVER 116. For each discrete time step the CPU of each of DEVICES 104-108 calculates a respective DSI associated with the relevant DEVICE. This DSI is compared with a corresponding DSI code that is calculated for that DEVICE by SIMULATOR 118. A mismatch between these values is an indication of, e.g., operational failure or of illegitimate reprogramming of SYSTEM 102.

[0022] \[ X_k(t) = F_k(X_1(t-1), X_2(t-1),..., X_M(t-1), S_k, X_k(t-2), X_k(t-3), X_k(t-4),..., X_k(t-N)) \]

is a mathematical expression defining an FSM. A value \( X_k(t) \) is calculated for each DEVICE \( k \) for each time step \( t \) according to this expression, wherein:

- "\( t \)" is the current moment in time;
- "\( k \)" is the index or label for DEVICE \( k \), running from 1 to \( M \), assuming the number of DEVICES equals \( M \) (\( M \) equals 3 in the illustrated example) in the PAN;
- "\( S_k \)" is the DSI of DEVICE \( k \); and
- "\( F_k \)" (\( \ldots \)) is the "\( k \)"-th component of a mathematical vector function chosen such that the set of \( M \) equations describes a stochastic non-periodical dynamic process.

[0023] Accordingly, \( X_k(t) \) for a fixed "\( k \)" depends on the values \( X \) of all DEVICES 104-108 taken at the previous time step, on the DSI of DEVICE \( k \), and on the history of the value \( X \) for DEVICE \( k \). The length of the history taken into account is determined by the number \( N \). SIMULATOR 118 calculates these values \( X_k(t) \) for all "\( k \)" in each time step using the same mathematical correspondence. When the user seeks access to a system (not shown) that requires a valid ID, one or more of the values \( X_k(t) \) as calculated by DEVICES 104-108 for the point in time "\( t \)" are compared with the relevant ones of the values \( X_k(t) \) as calculated by SIMULATOR 118 for the same point in time. A discrepancy is an indication that the user is not authorized or that the integrity of SYSTEM 102 has been violated.

[0024] At least one device on the PAN is enabled to communicate with CONTROL SERVER 116 directly or through a proxy (not shown). Preferably, the value \( X_k(t) \) is sent to the SERVER 116 along with the indication of the label \( k \) of the designated device, unless the label is pre-defined in the system. In order to increase the accuracy and security of the system, a sequence of generated values \( X_k(t=T_q) \) with one or more device labels "\( p \)" and optionally with one or more time stamps \( T_q \) are communicated to CONTROL SERVER 116. CONTROL SERVER 116 may pick any of the values \( X_p(t=T_q) \) in order to evaluate them against the results provided by SIMULATOR 118. Communications between the PAN and other networks can be encrypted using the value \( X_p(t=T_q) \) as a seed for the encryption key generator.

[0025] In order to reprogram any of DEVICES 104-108 or in order to issue some extra command directly and with effect on SYSTEM 102, a virus or a hacker has to penetrate all DEVICES 104-108 of SYSTEM 102 and has to collect the required history \( X_q(t-1), X_q(t-2),..., X_q(t-N) \) for all DEVICES 104-108. Due to the stochastic nature of the evolution of the model given by the set of equations of Fig.2, all these manipulations are to be performed during one time step. This makes undetected hacking or interfering with SYSTEM 102 technically and computationally a very complex task.

[0026] The set of FSMs forms a discrete system that can assume a finite number of possible system states. The states assumed in succession by the system can in principle be calculated via the above-mentioned deterministic equations. The sequence of states is therefore not truly stochastic, unless a stochastic variable is introduced into the mathematical relationship. For example, one or more of devices 104-108 may provide a stochastic value for a parameter taken into account in the development of the system by making one or more of the \( F_k \) depend on it. If device 104 comprises a cellphone, the value for the parameter is, e.g., the number of calls made or received over the last week, possibly weighted by the time intervals between the calls, and determined at the time the user needs an ID. If device 106 is a radio or an MP3 player, the value for the parameter is, e.g., a number determined by the content of a buffer for data played out. The expressions "stochastic" and "non-periodic stochastic" are therefore to be understood as also indicative of non-stochastic behavior that looks stochastic for practical purposes of this invention, e.g., for the lifetime of the application.

[0027] It should be noted that the above-mentioned embodiments illustrate rather than limit the invention, and that those skilled in the art will be able to design many alternative embodiments without departing from the scope of the appended claims. In the claims, any reference signs placed between parentheses shall not be construed as limiting the claim. The word "comprising" does not exclude the presence of elements or steps other than those listed in a claim. The word "a" or "an" preceding an element does not exclude the presence of a plurality of such elements. The invention can be implemented by means of hardware comprising several distinct elements, and by means of a suitably programmed computer. In the device claim enumerating several means, several of these means can be embodied by one and the same item of hardware. The mere fact that certain measures are recited in mutually different dependent claims does not indicate that a combination of these measures cannot be used to advantage.
1. A method of determining an ID value for a user, the method comprising the steps of:

   multiple devices (104, 106, 108) of a personal area network (102) of the user calculating the ID value in a distributed manner among the multiple devices (104, 106, 108);
   each of the multiple devices (104, 106, 108) comprising a respective finite state machine (112, 114, 110) used in the calculating of the ID value, wherein
   each respective finite state machine (112, 114, 110) calculates a respective ID value per time step; and
   each calculated respective ID value depends on a previous state of at least one of the other of the finite state machines (112, 114, 110).

2. The method of claim 1, wherein:

   a respective finite state machine (112, 114, 110) calculates per time step a value of a quantity according to a respective mathematical relationship having as arguments:
   the value of the quantity calculated at a preceding time step by at least another one of the finite state machines (112, 114, 110), and
   a respective history of values assumed by the quantity calculated by the respective finite state machine (112, 114, 110); and
   wherein the respective mathematical relationship is such that the quantity assumes a practically stochastic behaviour.

3. A personal appliance (104, 106, 108) for use in a personal area network (102); the personal appliance (104, 106, 108) configured to communicate with at least one other appliance (104, 106, 108) of the personal area network (102); characterised by:

   the personal appliance (104, 106, 108) comprising a finite state machine (112, 114, 110) and being adapted to take part in a determining of an ID value for a user;
   wherein the ID value for a user is determined according to the method of claim 1 or claim 2.

Patentansprüche

1. Verfahren zum Bestimmen eines ID-Wertes für einen Benutzer, wobei das Verfahren die Schritte aufweist:

   mehrere Vorrichtungen (104, 106, 108) eines Personal Area Networks (102) des Benutzers berechnen den ID-Wert in einer verteilten Weise zwischen den mehreren Vorrichtungen (104, 106, 108);
   wobei jede der mehreren Vorrichtungen (104, 106, 108) einen jeweiligen endlichen Zustandsautomaten (112, 114, 110) aufweist, der beim Berechnen des ID-Wertes verwendet wird, wobei
   jeder jeweilige endliche Zustandsautomat (112, 114, 110) einen jeweiligen ID-Wert pro Zeit schritt berechnet; und
   jeder berechnete jeweilige ID-Wert von einem vorherigen Zustand von zumindest einem der anderen der endlichen Zustandsautomaten (112, 114, 110) abhängt.

2. Verfahren gemäß Anspruch 2, wobei:

   ein jeweiliger endlicher Zustandsautomat (112, 114, 110) pro Zeitschritt einen Wert einer Größe gemäß einer jeweiligen mathematischen Beziehung berechnet, die als Argumente aufweist:
   den Wert der Größe berechnet zu einem vorhergehenden Zeitschritt durch zumindest einen anderen der endlichen Zustandsautomaten (112, 114, 110), und
   einen jeweiligen Verlauf von Werten, die durch die Größe angenommen werden, die durch den jeweiligen endlichen Zustandsautomaten (112, 114, 110) berechnet wird; und wobei
   die jeweilige mathematische Beziehung derart ist, dass die Größe ein praktisch stochastisches Verhalten annimmt.

3. Persönliches Gerät (104, 106, 108) zur Verwendung in einem Personal Area Network (102); wobei das persönliche Gerät (104, 106, 108) ausgebildet ist, mit zumindest einem anderen Gerät (104, 106, 108) des Personal Area Networks (102) zu kommunizieren; dadurch gekennzeichnet, dass:

   das persönliche Gerät (104, 106, 108) einen endlichen Zustandsautomaten (112, 114, 110) aufweist und eingerichtet ist, an einem Bestim men eines ID-Wertes für einen Benutzer teilzunehmen;
   wobei der ID-Wert für einen Benutzer gemäß dem Verfahren des Anspruchs 1 oder des Anspruchs 2 bestimmt wird.
Revendications

1. Procédé de détermination d’une valeur d’identifiant ID pour un utilisateur, le procédé comprenant les étapes suivantes :

   des dispositifs multiples (104, 106, 108) d’un réseau personnel (102) de l’utilisateur (102) calculant la valeur de l’identifiant ID d’une manière distribuée entre les dispositifs multiples (104, 106, 108) ;
   chacun des dispositifs multiples (104, 106, 108) comportant une machine à états finis (112, 114, 110) correspondante utilisée pour le calcul de la valeur de l’identifiant ID, dans lequel chaque machine à états finis correspondante (112, 114, 110) calcule une valeur respective de l’identifiant ID par étape temporelle ; et chaque valeur respective calculée de l’identifiant ID dépend d’un état précédent d’au moins une autre des machines à états finis (112, 114, 110).

2. Procédé selon la revendication 1, dans lequel :

   une machine à états finis correspondante (112, 114, 110) calcule par pas temporel une valeur d’une quantité selon une relation mathématique correspondante ayant comme arguments :

   la valeur de la quantité calculée lors d’un pas temporel précédent par au moins une des machines à états finis (112, 114, 110), et un historique correspondant des valeurs obtenues par la quantité calculée par les machines à états finis respectives (112, 114, 110) ; et dans lequel la relation mathématique correspondante est telle que la quantité a un comportement pratiquement aléatoire.

3. Appareil personnel (104, 106, 108) utilisable dans un réseau personnel (102) ;

   l’appareil personnel (104, 106, 108) étant configuré pour communiquer avec au moins un autre appareil personnel (104, 106, 108) du réseau personnel (102) caractérisé par le fait que :

   l’appareil personnel (104, 106, 108) comporte une machine à états finis (112, 114, 110) et est agencé de manière à prendre part à une détermination d’une valeur d’un identifiant ID pour un utilisateur ;

   dans lequel la valeur de l’identifiant ID pour un utilisateur est déterminée selon le procédé de la revendication 1 ou de la revendication 2.
REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader’s convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 5590199 A [0007]