(19) **Bundesrepublik Deutschland**
Deutsches Patent- und Markenamt

(10) **DE 600 38 617 T2** 2009.05.07

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 219 064 B1**
(21) Deutsches Aktenzeichen: **600 38 617.1**
(86) PCT-Aktenzeichen: **PCT/EP00/12405**
(96) Europäisches Aktenzeichen: **00 983 258.5**
(87) PCT-Veröffentlichungs-Nr.: **WO 2001/046784**
(86) PCT-Anmeldetag: **07.12.2000**
(87) Veröffentlichungstag der PCT-Anmeldung: **28.06.2001**
(97) Erstveröffentlichung durch das EPA: **03.07.2002**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **16.04.2008**
(47) Veröffentlichungstag im Patentblatt: **07.05.2009**

(51) Int Cl.[8]: ***H04L 9/32*** (2006.01)

(30) Unionspriorität:
469453 **21.12.1999** **US**

(84) Benannte Vertragsstaaten:
DE, FR, GB, NL

(73) Patentinhaber:
NXP B.V., Eindhoven, NL

(72) Erfinder:
SITNIK, Eran, NL-5656 AA Eindhoven, NL

(74) Vertreter:
Richter, Werdermann, Gerbaulet & Hofmann, 20354 Hamburg

(54) Bezeichnung: **VERFAHREN UND VORRICHTUNG ZUM AUTHENTIFIZIEREN VON ZEITABHÄNGIGEN INTERAKTIVEN ÜBERTRAGUNGEN**

Beschreibung

GEBIET DER ERFINDUNG

[0001] Die vorliegende Erfindung betrifft digitale Zeitstempelungstechniken, insbesondere ein Verfahren und eine Vorrichtung zum Authentifizieren von zeitabhängigen interaktiven Übertragungen, beispielsweise von Fernsehereignissen.

AUSGANGSSITUATION DER ERFINDUNG

[0002] Die Verwendung von öffentlichen oder quasiöffentlichen Netzen, beispielsweise das Internet, für potentiell sensitive oder geschützte elektronische Datenübertragen, beispielsweise E-Mail und elektronische Finanztransaktionen, nimmt rapide zu. Folglich besteht ein zunehmender Bedarf an verbesserten Computersicherheitstechniken, die die Privatsphäre oder Authentizität solcher elektronischer Übertragungen gewährleisten. Zum Autorisieren oder Authentifizieren solcher elektronischer Nachrichten oder der in ihnen enthaltenen Informationen und zum Gewährleisten, dass diese nicht geändert worden sind, sind eine Anzahl von Techniken vorgeschlagen oder empfohlen worden.

[0003] Bei vielen elektronischen Übertragungen ist es wichtig, die Zeit und/oder das Datum, die bzw. das mit einer Nachricht verknüpft ist/sind, zu verifizieren. Folglich sind Techniken zum Verknüpfen eines sicheren digitalen Zeitstempels mit einer elektronischen Nachricht zum Überprüfen der Gültigkeit der angegebenen Zeit- und Datumsinformationen entwickelt worden. Im Allgemeinen versuchen solche digitalen Zeitstempel zu verhindern, dass ein Benutzer das Datum einer/eines elektronischen Nachricht, Dokuments oder Transaktion ändert. Gemäß einem Lösungsansatz werden elektronische Dokumente durch einen unparteiischen Dritten, der oft als „digitaler Notar" bezeichnet wird, unterschrieben und mit einem Zeitstempel versehen.

[0004] Außerdem offenbart das US-Patent Nr. 5.001.752 an Fischer ein System, mit dem ein elektronisches Dokument oder eine elektronische Transaktion mit einem sicheren Zeitstempel versehen wird, ohne dass ein „digitaler Notar" notwendig ist. Eine allgemeine Erörterung geeigneter Verschlüsselungs- und Sicherheitstechniken finden Sie zum Beispiel in Applied Cryptography von B. Schneier (2. Ausgabe 1997).

[0005] Zwar hindern solche früheren Systeme, mit denen elektronische Dokumente oder Transaktionen mit einem digitalen Zeitstempel versehen werden, einen Benutzer erfolgreich daran, die/das absolute Zeit oder Datum des/der elektronischen Dokuments oder Transaktion zu ändern, doch ermöglichen sie nicht das Berechnen der Differenzzeit, die ein Benutzer benötigt, um auf ein bestimmtes Ereignis zu reagieren. Außerdem erfordern solche früheren Systeme, mit denen elektronische Dokumente oder Transaktionen mit einem digitalen Zeitstempel versehen werden, eine sehr genaue Synchronisierung zwischen dem zentralen Server und den verteilten Endbenutzergeräten.

[0006] Folglich besteht ein Bedarf an einem Verfahren und einer Vorrichtung zum Berechnen und Überprüfen der Gültigkeit der Zeit zwischen einem Ereignis, beispielsweise die Ankündigung einer Auktion oder eines Wettbewerbs in einer Fernsehsendung, und dem Zeitpunkt, zu dem ein Benutzer reagiert. Ferner besteht ein Bedarf an einem Verfahren und einer Vorrichtung zum Berechnen und Überprüfen der Gültigkeit der Zeit zwischen einem Ereignis und dem Zeitpunkt, zu dem ein Benutzer reagiert, mit gelockerten Synchronisierungsanforderungen.

ZUSAMMENFASSUNG DER ERFINDUNG

[0007] Im Allgemeinen werden ein Verfahren und eine Vorrichtung zum Berechnen und Überprüfen der Gültigkeit der Differenzzeit zwischen der Übertragung eines Ereignisses und dem Zeitpunkt, zu dem ein Benutzer reagiert, offenbart. Das Ereignis kann beispielsweise die Ankündigung einer Auktion oder eines Wettbewerbs in einer Fernsehsendung einschließen. Für eine veranschaulichende Fernsehwettbewerbsausführungsform bestimmt die vorliegende Erfindung die Zeit zwischen der ursprünglichen Präsentation des Wettbewerbs gegenüber dem Benutzer und dem Zeitpunkt, zu dem der Benutzer auf den Wettbewerb reagiert.

[0008] Die vorliegende Erfindung ermöglicht sichere, genaue und in Echtzeit ablaufende Mehrbenutzerereignisse. Die Differenzzeit für eine Endbenutzerreaktion wird durch das entsprechende Endbenutzergerät berechnet. Die Reaktion kann dann, zusammen mit der berechneten Differenzreaktionszeit, dem Provider sicher und zuverlässig in Echtzeit oder offline rückgemeldet werden. In einer Ausführungsform schließt jedes Endbenutzergerät eine sichere Zeitmesseinrichtung mit einer sicheren Uhr-/Datumsanzeigefunktion zum Berechnen der Differenzzeit zwischen der Präsentation des Ereignisses und der Benutzerreaktion ein. Die Verschlüsselungs- und Zeitstempelungsfunktionen der vorliegenden Erfindung können beispielsweise direkt in jedes Endbenutzergerät oder in eine Chipkarte oder ein anderes tragbares Gerät, das in das Endbenutzergerät eingeführt werden kann, integriert sein.

[0009] Ein anderer Aspekt der Erfindung verhindert die betrügerische Modifizierung der Differenzzeit. Es wird verhindert, dass ein Benutzer ein bestimmtes Ereignis aufzeichnet, beispielsweise unter Verwendung eines Videorekorders (VCR), und danach das aufge-

zeichnete Ereignis abspielt und auf das abgespielte Ereignis reagiert, wodurch er die tatsächliche Reaktionszeit ändert. Somit vergleicht die vorliegende Erfindung lokale und globale Präsentationszeitinformationen, um zu gewährleisten, dass jeder Benutzer auf das ursprüngliche, in Echtzeit ablaufende Ereignis und nicht auf die spätere Wiedergabe des Ereignisses reagiert.

[0010] Ein umfassenderes Verständnis der vorliegenden Erfindung sowie weitere Merkmale und Vorteile der vorliegenden Erfindung erlangt bzw. erfährt man unter Bezugnahme auf die folgende/n ausführliche Beschreibung und Zeichnungen.

KURZE BESCHREIBUNG DER ZEICHNUNGEN

[0011] Fig. 1 veranschaulicht eine Netzumgebung, in der die vorliegende Erfindung funktionieren kann;

[0012] Fig. 2 ist ein schematisches Blockdiagramm eines beispielhaften Senders, der zu einem Provider gehört, gemäß der vorliegenden Erfindung;

[0013] Fig. 3 veranschaulicht einen beispielhaften MPEG-Datenstrom (MPEG = Motion Pictures Expert Group) für eine beispielhafte Fernsehwettbewerbsimplementierung der vorliegenden Erfindung;

[0014] Fig. 4 ist ein schematisches Blockdiagramm eines beispielhaften Endbenutzergeräts gemäß der vorliegenden Erfindung; und

[0015] Fig. 5 ist ein Ablaufdiagramm, das einen beispielhaften Hintergrundereignisreaktionshandhabungsprozess beschreibt, der Prinzipien der vorliegenden Erfindung verkörpert und durch das Endbenutzergerät von Fig. 4 ausgeführt wird.

AUSFÜHRLICHE BESCHREIBUNG

[0016] Fig. 1 veranschaulicht eine Netzumgebung **100** zum Übertragen von Multimedia-Informationen, beispielsweise Videosignale, Audiosignale und Daten, von einem Provider, beispielsweise ein Fernsehsender, unter Verwendung eines weiter unten im Zusammenhang mit Fig. 2 erörterten Senders **200** zu einem oder mehreren Endbenutzern, die Endbenutzergeräte **400-1** bis **400-n** (im Folgenden insgesamt als Endbenutzergeräte **400** bezeichnet) verwenden, die weiter unten im Zusammenhang mit Fig. 4 erörtert werden. Die Endbenutzergeräte **400** können beispielsweise als digitale Fernsehgeräte (beispielsweise Philips Digital High Definition Television, Modell 64PH9905, im Handel erhältlich von Philips Electronics N. A.) ausgeführt sein.

[0017] Die Netzumgebung **100** kann beispielsweise als ein drahtloses Sendenetz, beispielsweise ein Mobiltelefonnetz, ein terrestrisches Fernsehsendenetz oder ein DDS-Fernsehnetz (DSS = Digital Satellite Service) oder ein drahtgebundenes Netz, beispielsweise das Internet, ein Fernsprechnetz (PSTN) oder ein Kabelfernsehnetz oder eine Kombination der vorgenannten Netze ausgeführt sein. Zwar ist die vorliegende Erfindung hierin im Kontext eines Fernsehwettbewerbs veranschaulicht, doch kann, wie einem Fachmann einleuchten würde, die vorliegende Erfindung auf jedes zeitabhängige Ereignis, bei dem mehrere Benutzer über ein Netz mit einem Provider kommunizieren, angewendet werden.

[0018] Gemäß einem Merkmal der vorliegenden Erfindung wird die Differenzzeit, die ein Benutzer benötigt, um auf ein bestimmtes Ereignis, beispielsweise die Ankündigung einer Auktion oder eines Wettbewerbs in einer Fernsehsendung, zu reagieren, sicher und zuverlässig durch jedes Endbenutzergerät **400** berechnet. Auf diese Weise ermöglicht die vorliegende Erfindung faire, sichere, genaue und in Echtzeit ablaufende Mehrbenutzerereignisse, beispielsweise Auktionen, Wettbewerbe, Spiele oder Abstimmungen. Typischerweise ist der relative Zeitraum von Interesse die tatsächliche Zeit, die ein Benutzer benötigt, um auf das Ereignis zu reagieren. So ist beispielsweise bei einem Fernsehwettbewerb der Zeitraum von Interesse die Zeit zwischen der ursprünglichen Präsentation des Wettbewerbs gegenüber dem Benutzer und dem Zeitpunkt, zu dem der Benutzer auf den Wettbewerb reagiert.

[0019] In einer Ausführungsform, die weiter unten erörtert wird, schließt jedes Benutzergerät **400** eine sichere Zeitmesseinrichtung ein, die eine sichere Uhr-/Datumsanzeigefunktion zum Berechnen der Differenzzeit zwischen der Präsentation des Ereignisses und der Benutzerreaktion einschließt. Da die vorliegende Erfindung die Differenzzeit für die Benutzerreaktion lokal und zuverlässig berechnet, kann die Reaktion zu einer beliebigen Zeit an den Sender **200** zurückgesendet werden, um beispielsweise die durch den Provider **200** empfangenen Nachrichten zu verteilen, oder zu Zeiten geringeren Netzverkehrs gesendet werden.

[0020] Gemäß einem anderen Merkmal der vorliegenden Erfindung wird ein Benutzer daran gehindert, ein bestimmtes Ereignis aufzuzeichnen, beispielsweise unter Verwendung eines Videorekorders (VCR), und danach das aufgezeichnete Ereignis abzuspielen und auf das abgespielte Ereignis zu reagieren und dadurch die tatsächliche Reaktionszeit zu ändern. Somit vergleicht die vorliegende Erfindung lokale und globale Präsentationszeitinformationen, um zu gewährleisten, dass jeder Benutzer auf das ursprüngliche, in Echtzeit ablaufende Ereignis und nicht auf die spätere Wiedergabe des Ereignisses reagiert.

[0021] Fig. 2 veranschaulicht einen beispielhaften

Sender **200**, der zu einem Provider **110** gehört, gemäß der vorliegenden Erfindung. Der Sender **200** kann zu einem Fernsehnetz, einem Kabelbetreiber, einem DSS-Betreiber oder einem beliebigen Provider, der Programminhalt sendet, gehören. Der Sender **200** schließt einen Prozessor **210** und einen damit in Beziehung stehenden Speicher, beispielsweise ein Datenspeicher **220**, ein. Der Prozessor **210** kann als einzelner Prozessor oder als eine Anzahl von parallel arbeitenden Prozessoren ausgeführt sein.

[0022] Der Datenspeicher **220** und/oder ein Nur-Lese-Speicher (ROM) sind/ist so betreibbar, dass sie/er einen oder mehrere Befehle speichern/speichert, und der Prozessor **210** ist so betreibbar, dass er diese/n abruft, interpretiert und ausführt. Außerdem schließt der Sender **200** vorzugsweise einen sicheren Memory Store **250** zum Aufzeichnen von Schlüsselinformationen auf bekannte Weise ein. Der sichere Memory Store **250** zeichnet alle notwendigen öffentlichen oder privaten Schlüsselinformationen auf und sollte nichtflüchtig und gegen unbefugte Eingriffe gesichert sein.

[0023] Außerdem schließt der Sender **200**, wie Fig. 2 zeigt, vorzugsweise einen Zufallszahlengenerator **260** und ein Taktgebermodul **270** ein. Der Zufallszahlengenerator **260** produziert eine Zufallszahl, die auf bekannte Weise bei Berechnungen von öffentlichen Schlüsseln verwendet werden kann. Wie weiter unten im Zusammenhang mit Fig. 3 erörtert wird, generiert das Taktgebermodul **270** Zeitstempelwerte, die mit den Ereignisdaten gesendet werden. Eine ausführlichere Erörterung der Verschlüsselungs- und Zeitstempelfunktionen des Senders **200** finden Sie zum Beispiel im US-Patent Nr. 5.001.752 an Fischer.

[0024] Der Übertragungsport **230** verbindet den Sender **200** mit dem Netz **100** und verbindet dadurch den Sender **200** mit jedem angeschlossenen Gerät, das in Fig. 1 gezeigt wird.

[0025] Fig. 3 veranschaulicht einen beispielhaften Datenstrom **300**, zum Beispiel einen MPEG-Strom (MPEG = Motion Pictures Expert Group) für eine beispielhafte Fernsehwettbewerbsimplementierung der vorliegenden Erfindung. Wie Fig. 3 zeigt, kann der MPEG-Datenstrom **300** Ereignissteuerdaten **310** einschließen, die durch den Sender **200** zusammen mit den Video- und Audiodaten **320**, **330** gesendet werden. Die Ereignissteuerdaten **310** können verschlüsselte Pakete einschließen, die die Optionen in dem Wettbewerb beschreiben. So schließen die in Fig. 3 gezeigten Ereignissteuerdaten **310** beispielsweise einen verschlüsselten globalen Zeitstempel (Datum/Zeit) **341**, eine Präsentationszeit (PTS) **342** relativ zu dem Systemzeittaktgeber (STS) des Gesamt-MPEG-Stroms **300**, einen Ereignisbezeichner **343** und, optional, eine korrekte Antwort **344** ein. Der globale Zeitstempel (Datum/Zeit) **341** ist der Zeitpunkt, zu dem das MPEG-Paket durch den Sender **200** gesendet wurde, und die Präsentationszeit (PTS) **342** ist die genaue Zeit, zu der das Endbenutzergerät **400** das Bild auf dem Anzeigegerät des Benutzers wiedergeben sollte. Es sei angemerkt, dass der MPEG-Datenstrom **300** in periodischen Abständen einen neuen öffentlichen Schlüssel gemäß wohlbekannten Techniken des bedingten Zugriffs einschließen kann.

[0026] Fig. 4 veranschaulicht ein beispielhaftes Endbenutzergerät **400** gemäß der vorliegenden Erfindung. Die Endbenutzergeräte **400** können beispielsweise als digitale Fernsehgeräte oder Personalcomputer ausgeführt sein. Das Endbenutzergerät **400** schließt einen Prozessor **410** und einen damit in Beziehung stehenden Speicher, beispielsweise ein Datenspeicher **420**, ein. Der Prozessor **410** und der Datenspeicher **420** funktionieren ähnlich wie der Prozessor **210** und der Datenspeicher **220**, die weiter oben im Zusammenhang mit Fig. 2 erörtert wurden.

[0027] Außerdem kann das Endbenutzergerät **400** vorzugsweise einen sicheren Memory Store **450** zum Aufzeichnen von Schlüsselinformationen auf bekannte Weise einschließen. Der sichere Memory Store **450** zeichnet alle notwendigen öffentlichen oder privaten Schlüsselinformationen auf und sollte nichtflüchtig und gegen unbefugte Eingriffe gesichert sein. Außerdem schließt der Endbenutzergerät **400**, wie Fig. 4 zeigt, vorzugsweise einen Zufallszahlengenerator **460** und ein Taktgebermodul **470** ein. Der Zufallszahlengenerator **460** produziert eine Zufallszahl, die auf bekannte Weise bei Berechnungen von öffentlichen Schlüsseln verwendet werden kann.

[0028] Wie weiter unten im Zusammenhang mit Fig. 5 erörtert wird, generiert das Taktgebermodul **470** Zeitstempelwerte, die zum Berechnen der Differenzzeit zwischen der Präsentationszeit und der Reaktionszeit eines Ereignisses gemäß der vorliegenden Erfindung verwendet werden. Eine ausführlichere Erörterung der Verschlüsselungs- und Zeitstempelfunktionen des Endbenutzergeräts **400** finden Sie zum Beispiel im US-Patent Nr. 5.001.752 an Fischer. Es sei angemerkt, dass die Verschlüsselungs- und Zeitstempelfunktionen des Endbenutzergeräts **400** beispielsweise in eine Chipkarte oder ein anderes tragbares Gerät, das in das Endbenutzergerät **400** eingeführt wird, integriert sein können.

[0029] Der Übertragungsport **430** verbindet das Endbenutzergerät **400** mit dem Netz **100** und verbindet dadurch das Endbenutzergerät **400** mit jedem angeschlossenen Gerät, das in Fig. 1 gezeigt wird.

[0030] Der in Fig. 3 gezeigte MPEG-Datenstrom **300** kommt an jedem Endbenutzergerät **400** an. Das Endbenutzergerät **400** entschlüsselt die Ereignis-

steuerdaten **310** und zeichnet die Informationen in einer Ereignistabelle **425** auf. Somit werden der globale Zeitstempel (Datum/Zeit) **341**, die Präsentationszeit (PTS) **342**, der Ereignisbezeichner **343** und, optional, die korrekte Antwort **344** in den entsprechenden Feldern der Ereignistabelle **425** aufgezeichnet.

[0031] Das Endbenutzergerät **400** schließt einen im Zusammenhang mit Fig. 5 erörterten Hintergrundereignisreaktionshandhabungsprozess **500** ein, der während des Schritts **510** nach dem Empfang einer Benutzereingabe aktiviert wird. In einer alternativen Implementierung kann der Hintergrundereignisreaktionshandhabungsprozess **500** auf jedes Ereignis speziell zugeschnitten und mit dem MPEG-Datenstrom **300** in Form einer Steueranwendung, zum Beispiel ein Java-Applet, heruntergeladen werden. Der Empfänger **400** setzt das Abspielen der in dem MPEG-Strom eingeschlossenen Audio-/Videoinformationen **320**, **330** auf herkömmliche Weise während der Ausführung des Hintergrundereignisreaktionshandhabungsprozesses **500** fort.

[0032] Wie Fig. 5 zeigt, erlangt der Hintergrundereignisreaktionshandhabungsprozess **500** nach dem Erfassen eines Ereignisses die Präsentationszeit (PTS) **342** und den Ereignisbezeichner **343** aus den MPEG-Ereignissteuerdaten **310** und erlangt einen lokalen Zeitstempel der Ereignispräsentation von dem Taktgebermodul **470** während des Schritts **510**. Danach überwacht der Hintergrundereignisreaktionshandhabungsprozess **500** während des Schritts **515** die Benutzeraktionen, bis eine Benutzerreaktion empfangen worden ist. Sobald während des Schritts **515** eine Benutzerreaktion erfasst worden ist, erlangt der Hintergrundereignisreaktionshandhabungsprozess **500** einen lokalen Zeitstempel der Benutzerreaktion von dem Taktgebermodul **470** während des Schritts **520**.

[0033] Der Hintergrundereignisreaktionshandhabungsprozess **500** berechnet dann während des Schritts **525** die Differenzzeit zwischen den lokalen Zeitstempeln der Ereignispräsentation und der Benutzerreaktion.

[0034] Um noch mehr Sicherheit zu bieten (um zu verhindern, dass auf später wiedergegebene Ereignisse reagiert wird) berechnet der Hintergrundereignisreaktionshandhabungsprozess **500** außerdem während des Schritts **530** die Verzögerungszeit zwischen dem globalen Zeitstempel **341** des Senders und dem während des Schritts **510** von dem Taktgebermodul erlangten lokalen Zeitstempel der Ereignispräsentation. Es sei angemerkt, dass die Präsentationszeit (PTS) **342** während des Schritts **530** anstelle des oder zusätzlich zu dem globalen Zeitstempel/s **341** des Senders verwendet werden kann.

[0035] Dann wird während des Schritts **540** ein Test durchgeführt, um festzustellen, ob die in dem vorhergehenden Schritt berechnete Verzögerungszeit innerhalb einer vordefinierten Toleranz liegt. Im Allgemeinen wird die vordefinierte Toleranz bestimmt, indem Werte der durchschnittlichen Verzögerung durch das Netz **100** hindurch einfaktorisiert werden, und sie soll verhindern, dass ein Benutzer Zeit für die Reaktion auf ein später wiedergegebenes Ereignis hat. Wenn während des Schritts **540** festgestellt wird, dass die Verzögerungszeit den Schwellenwert überschreitet, wird während des Schritts **545** ein Verstoß gegen die Sicherheit erfasst. Es sei angemerkt, dass das Erfassen eines Verstoßes gegen die Sicherheit während der Schritte **540** und **545** durch den sicheren Empfänger **400** ausgeführt und für den Provider **200** gekennzeichnet (siehe Fig. 5) oder durch den Provider **200** erfasst werden kann.

[0036] Wenn jedoch während des Schritts **540** festgestellt wird, dass die Verzögerungszeit den Schwellenwert überschreitet, sendet der Ereignisreaktionshandhabungsprozess **500** während des Schritts **550** ein verschlüsseltes Reaktionspaket an den Sender **200**, das die während des Schritts **520** berechnete Differenzzeit, die Antwort und den Ereignisbezeichner enthält. In einer Ausführungsform, bei der die Ereignissteuerdaten **310** die korrekte Antwort enthalten, kann der während des Schritts **540** erfolgende Sendeschritt dahin gehend bedingt sein, ob die Antwort korrekt ist, oder es kann eine andere geeignete Nachricht an den Provider **200** gesendet werden. Es sei ferner angemerkt, dass die während des Schritts **550** gesendete Nachricht zeitverzögert sein kann, um die durch den Provider **200** empfangenen Nachrichten zu verteilen, oder zu Zeiten geringeren Netzverkehrs gesendet werden kann.

[0037] Nach dem Empfang der Antwortnachricht entschlüsselt der Provider **200** die Nachricht und vergleicht die empfangenen Differenzzeit- und Antwortinformationen mit aufgezeichneten Informationen für das gekennzeichnete Ereignis, um einen Gewinner zu kennzeichnen oder anderweitig die Gültigkeit der Zeit, die der Benutzer für das Reagieren benötigte, zu überprüfen.

[0038] Es versteht sich, dass die hierin gezeigten und beschriebenen Ausführungsformen und Variationen die Prinzipien dieser Erfindung lediglich veranschaulichen und dass durch Fachleute verschiedene Modifizierungen implementiert werden können, ohne vom Schutzbereich der Erfindung abzuweichen.

Bezugszeichenliste

Fig. 1

100 Netzumgebung
200 Sender
400-1 Benutzergerät
400-2 Benutzergerät
400-n Benutzergerät

Fig. 2

100 zum Netz
200 Sender
210 Prozessor
220 Datenspeicher
230 Übertragungsport
250 sicherer Memory Store
260 Zufallszahlengenerator
270 Taktgebermodul

Fig. 3

310 Ereignissteuerdaten
320 Videodaten
330 Audiodaten
341 globaler Zeitstempel
342 Präsentationszeit
343 Ereignisbezeichner
344 korrekte Antwort

Fig. 4

100 zum Netz
400 Endbenutzergerät
410 Prozessor
420 Datenspeicher
425 Ereignistabelle
430 Übertragungsport
450 sicherer Memory Store
460 Zufallszahlengenerator
470 Taktgebermodul
500 Ereignisreaktionshandhabungsprozess

Fig. 5 (von oben nach unten)

Ereignisreaktionshandhabungsprozess
510 Erlange Präsentationszeit (PTS) **342**, Ereignisbezeichner **343** und Zeitstempel der Ereignispräsentation von dem lokalen Taktgebermodul **470**.
515 Benutzerreaktion empfangen?
520 Erlange Zeitstempel der Benutzereingabe von dem lokalen Taktgebermodul **470** und zeichne globalen Zeitstempel **341** des Senders auf.
525 Berechne Differenzzeit zwischen den lokalen Zeitstempeln der Ereignispräsentation und der Benutzereingabe.
530 Berechne Verzögerungszeit zwischen dem globalen Zeitstempel **341** des Senders und dem lokalen Zeitstempel der Ereignispräsentation.
540 Verzögerungszeit innerhalb vordefinierten Wertes?
Yes Ja
No Nein
545 Erfasse und melde Verstoß gegen Sicherheit.
550 Verschlüssele und sende Paket, das die während des Schritts **520** berechnete Differenzzeit, die Antwort und den Ereignisbezeichner enthält, an Sender **200**.
Ende

Patentansprüche

1. Ein Verfahren zum Bestimmen des Betrages der Zeit zwischen einem gesendeten Ereignis und einer Benutzerreaktion, umfassend die folgenden Schritte:
Präsentieren besagten gesendeten Ereignisses gegenüber besagtem Benutzer zu einer verknüpften Präsentationszeit,
Bestimmen einer lokalen Reaktionszeit, zu der besagter Benutzer auf besagtes gesendetes Ereignis reagiert, unter Verwendung einer sicheren Taktquelle (**470**), die in dem entsprechenden Endbenutzergerät (**400**) eingeschlossen ist, und
Berechnen einer Differenzzeit zwischen besagter Präsentationszeit und besagter lokaler Reaktionszeit.

2. Das Verfahren nach Anspruch 1, ferner umfassend den Schritt des Sendens einer Nachricht an einen Provider besagten gesendeten Ereignisses einschließlich besagter Differenzzeit.

3. Das Verfahren nach Anspruch 2, wobei besagter Schritt des Sendens einer Nachricht an einen Provider besagten gesendeten Ereignisses zeitverzögert ist.

4. Das Verfahren nach Anspruch 2, wobei besagte Nachricht verschlüsselt ist.

5. Das Verfahren nach Anspruch 2, wobei besagte Nachricht besagte Reaktion einschließt.

6. Das Verfahren nach Anspruch 2, wobei besagte Nachricht einen Bezeichner besagten Ereignisses einschließt.

7. Das Verfahren nach Anspruch 1, wobei besagte sichere Taktquelle in einem tragbaren Gerät, das in das Endbenutzergerät eingeführt wird, eingeschlossen ist.

8. Das Verfahren nach Anspruch 1, wobei besag-

te Präsentationszeit aus Steuerdaten erlangt wird, die mit besagtem gesendeten Ereignis verknüpft sind.

9. Das Verfahren nach Anspruch 1, wobei besagte Präsentationszeit aus einem lokalen Zeitstempel erlangt wird, der nach der Präsentation besagten Ereignisses gegenüber besagtem Benutzer aktiviert wird.

10. Das Verfahren nach Anspruch 1, ferner umfassend den Schritt des Vergleichens einer lokalen Präsentationszeit und einer globalen Präsentationszeit, um zu gewährleisten, dass besagte Reaktion eine Echtzeitreaktion auf besagtes gesendetes Ereignis ist.

11. Das Verfahren nach Anspruch 10, ferner umfassend den Schritt des Sendens einer Nachricht an einen Provider besagten gesendeten Ereignisses einschließlich besagter Differenzzeit.

12. Das Verfahren nach Anspruch 11, wobei besagter Schritt des Sendens einer Nachricht an einen Provider besagten gesendeten Ereignisses zeitverzögert ist.

13. Das Verfahren nach Anspruch 11, wobei besagte Nachricht verschlüsselt ist.

14. Das Verfahren nach Anspruch 11, wobei besagte Nachricht besagte Reaktion einschließt.

15. Das Verfahren nach Anspruch 11, wobei besagte Nachricht einen Bezeichner besagten Ereignisses einschließt.

16. Das Verfahren nach Anspruch 10, wobei besagte sichere Taktquelle in einem tragbaren Gerät, das in das Endbenutzergerät eingeführt wird, eingeschlossen ist.

17. Das Verfahren nach Anspruch 10, wobei besagte Präsentationszeit aus Steuerdaten erlangt wird, die mit besagtem gesendeten Ereignis verknüpft sind.

18. Das Verfahren nach Anspruch 10, wobei besagte Präsentationszeit aus einem lokalen Zeitstempel erlangt wird, der nach der Präsentation besagten Ereignisses gegenüber besagtem Benutzer aktiviert wird.

19. Das Verfahren nach Anspruch 10, wobei besagter Schritt des Vergleichens gewährleistet, dass besagter Benutzer nicht auf eine spätere Wiedergabe besagten Ereignisses reagiert.

20. Ein System zum Bestimmen des Betrages der Zeit zwischen einem gesendeten Ereignis und einer Benutzerreaktion, umfassend:
eine sichere Taktquelle (**470**),
einen Speicher (**420**) zum Speichern eines maschinenlesbaren Codes und
einen Prozessor (**410**), der mit besagtem Speicher in Wirkverbindung steht, wobei besagter Prozessor so konfiguriert ist, dass er:
besagtes gesendetes Ereignis besagtem Benutzer zu einer verknüpften Präsentationszeit präsentiert,
eine lokale Reaktionszeit, zu der besagter Benutzer auf besagtes gesendetes Ereignis reagiert, unter Verwendung besagter sicherer Taktquelle (**470**) bestimmt und
eine Differenzzeit zwischen besagter Präsentationszeit und besagter lokaler Reaktionszeit berechnet.

21. Das System nach Anspruch 20, wobei besagter Prozessor ferner so konfiguriert ist, dass er eine lokale Präsentationszeit und eine globale Präsentationszeit vergleicht, um zu gewährleisten, dass besagte Reaktion eine Echtzeitreaktion auf besagtes gesendetes Ereignis ist.

Es folgen 3 Blatt Zeichnungen

Anhängende Zeichnungen

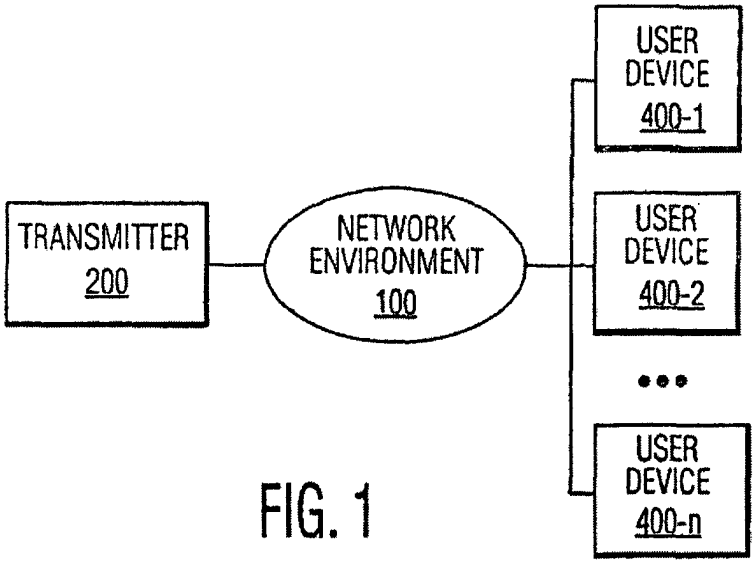

FIG. 1

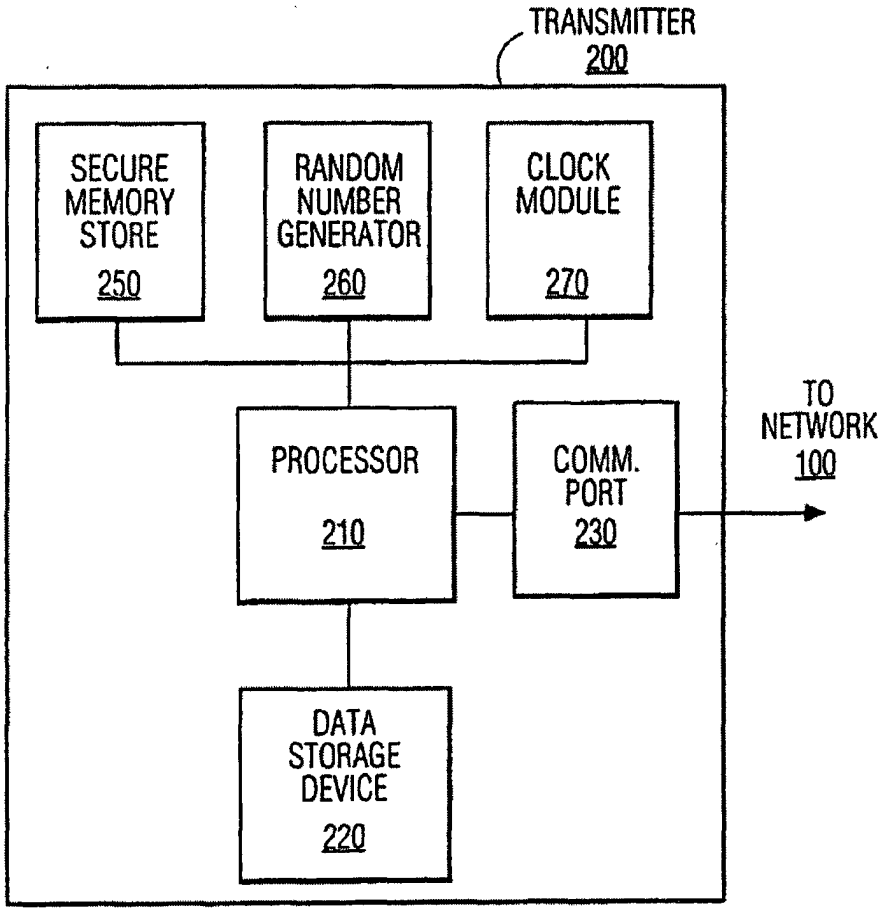

FIG. 2

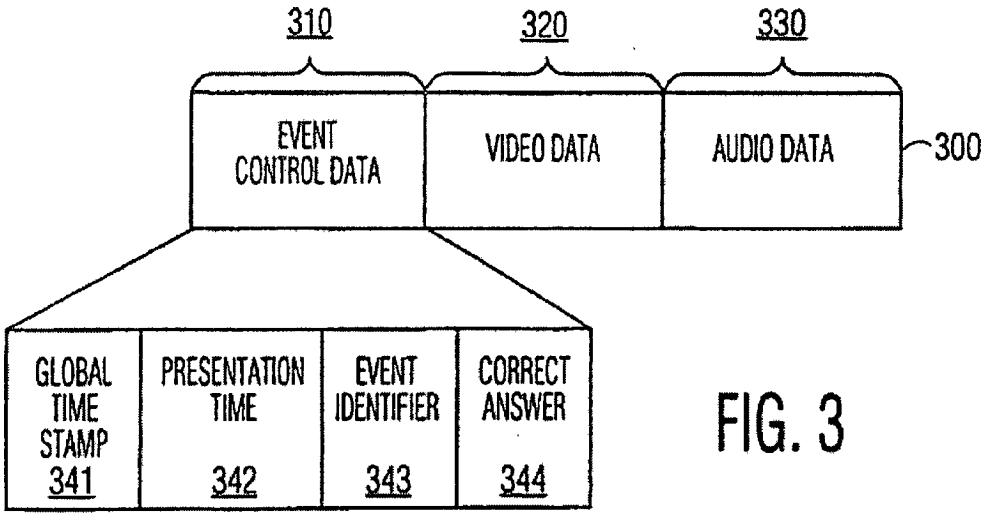
310
320
330
EVENT CONTROL DATA
VIDEO DATA
AUDIO DATA
300
GLOBAL TIME STAMP 341
PRESENTATION TIME 342
EVENT IDENTIFIER 343
CORRECT ANSWER 344

FIG. 3

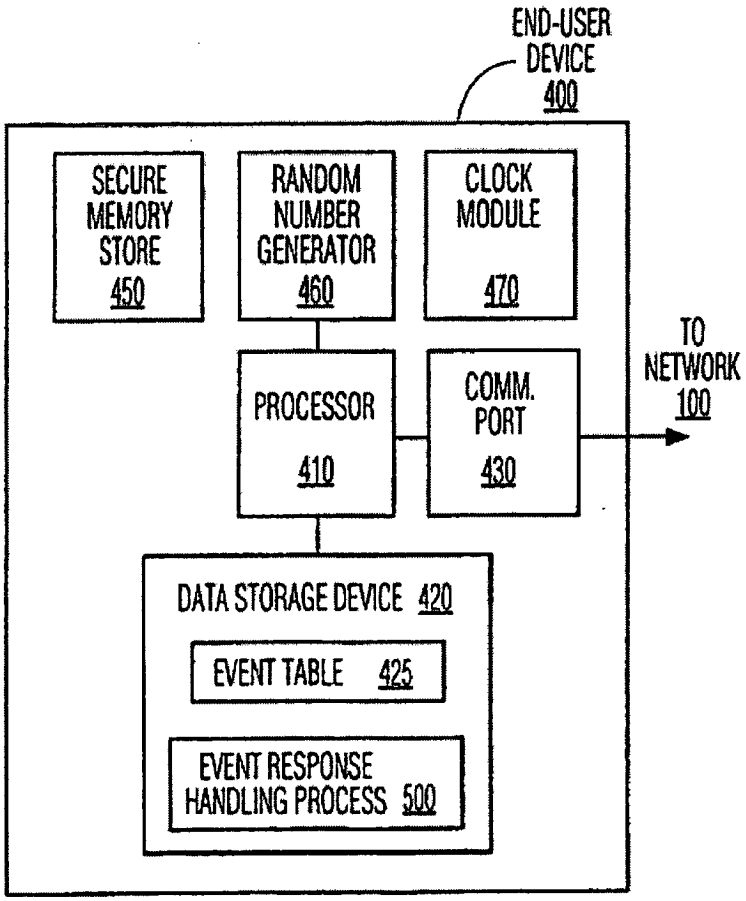
END-USER DEVICE 400
SECURE MEMORY STORE 450
RANDOM NUMBER GENERATOR 460
CLOCK MODULE 470
PROCESSOR 410
COMM. PORT 430
TO NETWORK 100
DATA STORAGE DEVICE 420
EVENT TABLE 425
EVENT RESPONSE HANDLING PROCESS 500

FIG. 4

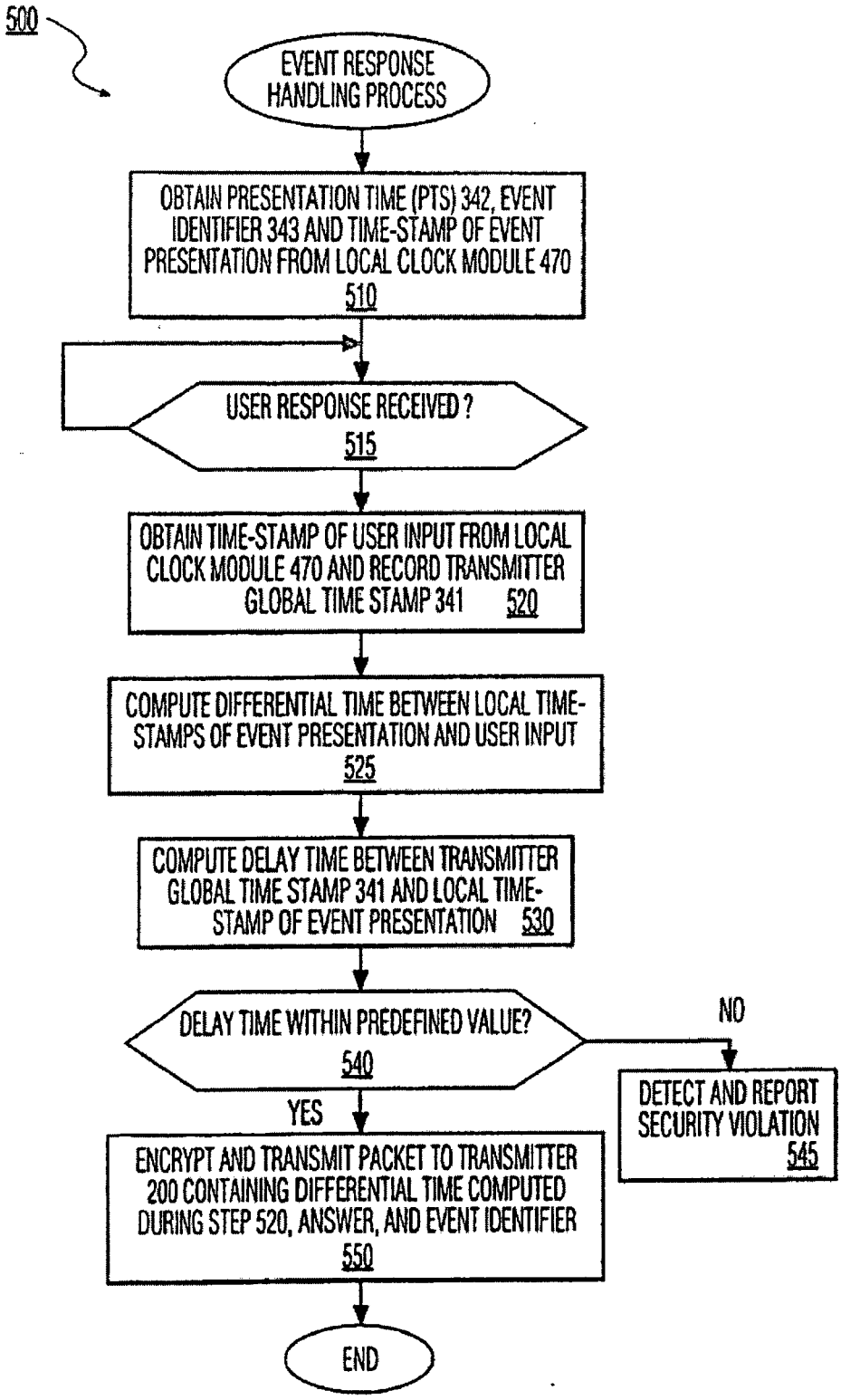
500
EVENT RESPONSE HANDLING PROCESS
OBTAIN PRESENTATION TIME (PTS) 342, EVENT IDENTIFIER 343 AND TIME-STAMP OF EVENT PRESENTATION FROM LOCAL CLOCK MODULE 470
510
USER RESPONSE RECEIVED ?
515
OBTAIN TIME-STAMP OF USER INPUT FROM LOCAL CLOCK MODULE 470 AND RECORD TRANSMITTER GLOBAL TIME STAMP 341
520
COMPUTE DIFFERENTIAL TIME BETWEEN LOCAL TIME-STAMPS OF EVENT PRESENTATION AND USER INPUT
525
COMPUTE DELAY TIME BETWEEN TRANSMITTER GLOBAL TIME STAMP 341 AND LOCAL TIME-STAMP OF EVENT PRESENTATION
530
DELAY TIME WITHIN PREDEFINED VALUE?
540
NO
DETECT AND REPORT SECURITY VIOLATION
545
YES
ENCRYPT AND TRANSMIT PACKET TO TRANSMITTER 200 CONTAINING DIFFERENTIAL TIME COMPUTED DURING STEP 520, ANSWER, AND EVENT IDENTIFIER
550
END

FIG. 5