

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2007-336558

(P2007-336558A)

(43) 公開日 平成19年12月27日 (2007. 12. 27)

(51) Int. Cl.		F I		テーマコード (参考)
H04L 9/32	(2006.01)	H04L 9/00	675A	5B285
G06F 21/20	(2006.01)	G06F 15/00	330A	5J104

審査請求 未請求 請求項の数 10 O L (全 9 頁)

(21) 出願番号 特願2007-157637 (P2007-157637) (22) 出願日 平成19年6月14日 (2007. 6. 14) (31) 優先権主張番号 06290992.4 (32) 優先日 平成18年6月16日 (2006. 6. 16) (33) 優先権主張国 欧州特許庁 (EP)	(71) 出願人 501263810 トムソン ライセンシング Thomson Licensing フランス国, エフ-92100 ブロー ニュ ビヤンクール, ケ アルフォンス ル ガロ, 46番地 46 Quai A. Le Gallo , F-92100 Boulogne- Billancourt, France (74) 代理人 100070150 弁理士 伊東 忠彦 (74) 代理人 100091214 弁理士 大貫 進介 (74) 代理人 100107766 弁理士 伊東 忠重 最終頁に続く
---	---

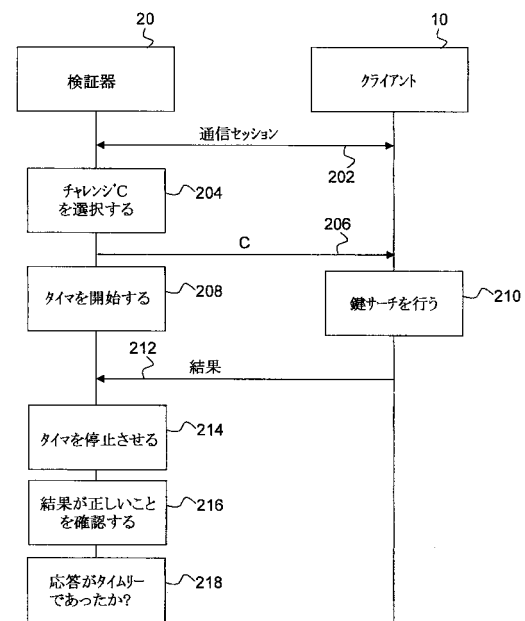
(54) 【発明の名称】 エミュレートされたクライアントを発見する高精度非サイクル測定を用いた装置及び方法

(57) 【要約】

【課題】 エミュレートされたクライアントを発見する方法。

【解決手段】 検証器 (20) が、暗号チャレンジCをクライアント (10) に送出し (206)、タイマー (22) を開始する (208)。クライアント (10) は、正しい鍵を求めるために決定論的鍵サーチ・アルゴリズムを用い (210)、必要な試行の数としてその結果を返す (212)。検証器 (20) は次いで、タイマー (22) を停止させ (214)、結果が正しいことを検証し (216)、応答がタイムリーであったことを検証する (218)。検証器 (20) も提供する。

【選択図】 図2



【特許請求の範囲】

【請求項 1】

クライアント（10）がエミュレートされているかを発見する方法であって、
チャレンジを前記クライアント（10）に送出する工程であって、解くために決定論的な数の反復を前記チャレンジが必要とする工程と、

前記数の反復を備えた応答（212）を受信すると、前記応答における前記反復の数が反復の期待数に一致した場合、前記クライアント（10）はエミュレートされていないと判定する工程（216、218）とを備える方法。

【請求項 2】

請求項 1 記載の方法であって、前記チャレンジの送出と応答の受信との間の時間を測定する工程（208、214）を更に備えており、前記判定する工程が、前記応答がタイムリーであったことを検証する工程を更に備える方法。 10

【請求項 3】

請求項 1 記載の方法であって、前記チャレンジは、前記クライアント（10）の識別情報又は前記クライアント（10）のユーザの識別情報に依存している方法。

【請求項 4】

請求項 1 記載の方法であって、前記チャレンジが暗号チャレンジである方法。

【請求項 5】

請求項 4 記載の方法であって、前記暗号チャレンジが鍵サーチである方法。

【請求項 6】

請求項 5 記載の方法であって、前記暗号チャレンジが、値の非暗号化バージョンと、前記値の暗号化バージョンと、前記鍵サーチにおいて第 1 の鍵が用いるための基底とを備える方法。 20

【請求項 7】

クライアント（10）がエミュレートされているかを発見する検証器（20）であって、

チャレンジを前記クライアント（10）に送出し、前記クライアントから応答（212）を受信する通信インタフェース（24）であって、解くために決定論的な数の反復を前記チャレンジが必要とし、前記応答（212）は前記反復の数を備えている通信インタフェースと、 30

前記チャレンジを選択し、

前記応答内の反復の数が反復の期待数に一致する場合に、前記クライアント（10）がエミュレートされていないことを判定する（216）、
プロセッサとを備える検証器。

【請求項 8】

請求項 7 記載の検証器であって、前記チャレンジの送出と前記応答の受信との間の時間を測定するタイマ（22）を更に備えており、前記プロセッサを、前記応答もタイムリーである場合に前記クライアント（10）がエミュレートされていないことを判定するよう適合させた検証器。 40

【請求項 9】

請求項 7 記載の検証器であって、前記プロセッサを、前記クライアント（10）の識別情報又は前記クライアント（10）のユーザの識別情報に前記チャレンジを依存させるよう適合させた検証器。 40

【請求項 10】

請求項 7 記載の検証器であって、前記プロセッサを、値の非暗号化バージョン、前記値の暗号化バージョン、及び前記鍵サーチにおいて第 1 の鍵が用いるための基底を備える暗号鍵サーチ・チャレンジであるチャレンジを選択するよう適合させた検証器。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、一般にセキュア・ネットワークに関し、特に前述のネットワークにおける装置の認証に関する。

【背景技術】

【0002】

クライアントにサービスを提供するサーバを有することがネットワークにおいて非常に一般的である。通常はユーザにあるクライアントはサービスをサーバから要求する。このサーバは、通常、サービスにアクセスする権利をクライアントが有している旨の検証後にサービスをクライアントに提供する。前述のサービスの例には、ビデオオンデマンド、文書の印刷、及び施錠されたドアの開錠がある。

【0003】

残念ながら、前述のサービスへのアクセスを得ることを、そうする権利を有することなしに試行する人々（いわゆる「ハッカー」や「海賊」）が存在している。この目的で、前述の人々は、ネットワーク内のセキュリティ解決策をだしぬくために種々の手法を用いる。

【0004】

ハッカーの活動をくじこうとする解決策の1つに認証がある。すなわち、サーバは、真のクライアントであることを確実にするためにクライアントを認証する。認証は、有効な、又は署名された識別情報の提示、ユーザ名及び関連したパスワードの提示、又は対称暗号法又は非対称暗号法が関係するプロトコルを用いて行うことができる。

【0005】

別の解決策は、特定のネットワーク内に受信装置があることを確実にすることである。例えば、欧州特許第1650671号明細書には、適切な応答を算出する受信器に、ランダムなチャレンジを送信器が送出するシステムが開示されている。次いで、送信器は、応答を戻すよう受信器に指示し、応答の受信までの時間を算出する。しかし、前述の解決策は、受信器までの距離を送信器が算出することを可能にするだけであるが、受信器の特性（送信器が事情により通じていなくても十分エミュレートすることができる）に関しては全く確実性を与えない。

【0006】

更に別の解決策は、その秘密を回復するか又はその挙動を修正するためにリバースエンジニアリングすることが難しいそのクローズド・プラットフォームを用いることである。認証などの他の解決策とともに通常用いるこの解決策は例えば、ゲーム・ステーション（例えば、プレイステーションやXボックス）、有料TVシステムのセットトップ・ボックス、トリプルプレイ・モデム（例えば、フリーボックスやライブボックス）や携帯電話機に用いられている。これは当然、アーキテクチャの多様性にその強みが起因するといえることができるパソコン（PC）とはかなり異なる。

【0007】

サーバを模倣するのに十分であるようにクローズド・プラットフォームをエミュレートすることが難しい一方、これが不可能でないことが明らかになった。この課題に対する標準的な解決策は取り消しである。クライアントが破られたことをシステム権限が知った場合、そのクライアントは、取り消しリストに載せられる。認証中、サーバはまず、クライアントが取り消しリストに載っているかを検証し、肯定の場合、サービスを拒否する。

【0008】

取り消しが効率的であるには、システム権限は、装置が破られたことを知っている必要がある。このことには長い時間がかかり得る。この間、ハッカーは、サービスを享受し続けるか、又は、更に悪いことには、多くの人々がサービスを利用することができるように装置をエミュレートする方法を他の人々に知らせることができる。

【0009】

この課題に対する解決策は、例えば、実行時間を測定することによってクライアントのフィンガープリンティングを行うことである。前述の種類のフィンガープリンティングは、エミュレートされたクライアントが、本物のプラットフォーム上のクライアントよりも

10

20

30

40

50

遅いことを前提とする。しかし、プロセッサがなお一層高速化するにつれ、このことは、依存する対象の前提ではない（特に特定の年齢のプラットフォームの場合）。

【発明の開示】

【発明が解決しようとする課題】

【0010】

よって、現行のセキュリティ解決策を改良し、エミュレートされた装置の検出をそれによってより容易にする解決策に対する必要性が存在している。

【課題を解決するための手段】

【0011】

本発明は前述の解決策を提供する。

10

【0012】

第1の局面では、本発明は、クライアントがエミュレートされたかを発見する方法に関する。解くために決定論的な数の反復を必要とするチャレンジがクライアントに送出される。上記数の反復を備えた応答を受信すると、応答における反復の数が反復の期待数に一致した場合、クライアントはエミュレートされていないと判定される。

【0013】

好ましい実施例では、チャレンジの送出と応答の受信との間の時間が測定され、応答がタイムリーであることをやはり前提とすれば、クライアントがエミュレートされていないことが判定される。

【0014】

20

好ましい実施例では、チャレンジは、クライアントの識別情報又はクライアントのユーザの識別情報に依存している。

【0015】

別の好ましい実施例では、チャレンジは暗号チャレンジであり、効果的には鍵サーチである。暗号チャレンジが、値の非暗号化バージョンと、値の暗号化バージョンと、鍵サーチにおいて第1の鍵が用いるための基底とを備えることは特に有利である。

【0016】

第2の局面では、本発明は、クライアントがエミュレートされたかを発見する検証器に関する。検証器は、クライアントにチャレンジを送出する通信インタフェースを備える。チャレンジは、解くために決定論的な数の反復を必要とする。インタフェースは、上記反復数を備えた応答をクライアントからの受信するためでもある。検証器は、チャレンジを選択し、応答内の反復数が、反復の期待数に一致する場合に、クライアントがエミュレートされていないことを判定するプロセッサを更に備える。

30

【0017】

好ましい実施例では、検証器は、チャレンジの送出と応答の受信との間の時間を測定するタイマも備え、プロセッサは、クライアントがエミュレートされていないことを判定するために、応答がタイムリーであったことを検証するようにも適合させる。

【0018】

好ましい実施例では、プロセッサは、クライアントの識別情報又はクライアントのユーザの識別情報にチャレンジを依存させるよう適合させる。

40

【0019】

更に別の好ましい実施例では、値の非暗号化バージョン、その値の暗号化バージョン、及び鍵サーチにおいて第1の鍵が用いるための基底を備える暗号鍵サーチ・チャレンジであるチャレンジを選択するよう適合させる。

【発明を実施するための最良の形態】

【0020】

本発明の好ましい実施例を、例として、添付図面を参照して次に説明する。

【実施例】

【0021】

図1は、互いに相互作用するよう適合させたクライアント10及び検証器20を示す。

50

クライアント 10 は、プロセッサ (CPU) 11 と、プロセッサ 11 によって実行されるアプリケーションを記憶するよう適合させたメモリ 13 と、装置、特に検証器 20 とネットワーク 1 を介して通信するよう適合させた通信インタフェース (I/O) 14 とを備える。検証器 20 は、プロセッサ (CPU) 21 と、プロセッサ 21 専用のタイマ 22 と、プロセッサ 21 によって用いるメモリ 23 と、装置、特にクライアント 10 とネットワーク 1 を介して通信するよう適合させた通信インタフェース (I/O) 24 とを備える。

【0022】

図 2 は、本発明の好ましい実施例によって、クライアントが、特定のプラットフォーム上で実行する (すなわち、エミュレートされていない) ことを検証する方法の好ましい実施例を示す。クライアント 10 が特定のプラットフォーム上で実行することを検証器 20 が検証したい場合、クライアント 10 との通信セッションを開設する (202)。検証器は次いで、クライアント 10 の暗号チャレンジ C を好ましくはランダムに選択する (204)。暗号チャレンジ C は、暗号関数を用いて (好ましくは、鍵長が 128 ビットの高度暗号化標準 (AES) アルゴリズムに基づいて) 計算される。好ましい実施例では、暗号チャレンジ C は、(clear, start, {clear}_{start+tries}) として表すことができる。ここで、clear は乱数、start は、暗号チャレンジ C の始点として用いられる乱数、tries は、クライアント 10 によって行う対象の試行の数である。すなわち、start+tries が、暗号チャレンジ C を破るための終点として用いられる。

【0023】

{clear}_{start+tries} は、鍵数 start+tries を備えた clear の暗号化の結果である。これは、暗号チャレンジ C の暗号化メッセージである。

【0024】

検証器 20 は、選ばれた暗号チャレンジ C をクライアント 10 に送出し (206)、タイマ 22 を開始する (208)。暗号チャレンジ C を受信すると、クライアント 10 はこれをそのメモリ 13 に記憶し、所定のアルゴリズムに従って、正しい鍵が求められるまで鍵を順次試行して、決定論的鍵サーチを行う (210)。好ましい鍵サーチ・アルゴリズムでは、

1. 試行カウンタ i=1 を初期化する
2. {clear}_{start+i} を計算する
3. 結果が {clear}_{start+tries} に等しいか否かを確認する
- 4a. 肯定の場合、暗号チャレンジ C が破られた結果として i を検証器 20 に送付する (212)
- 4b. 否定の場合、i を増やし、工程 2 に進む。

【0025】

多くの変形 (例えば、i を修正するための単純な増加よりも複雑な関数を用いることなど) が可能である。別の実施例において、工程 4a では、クライアント 10 は更に、検証器 20 に対するメッセージにおいて、正しい鍵を含める。

【0026】

別の好ましい実施例では、暗号チャレンジ C は、(clear, K_{start}, {clear}_{K=H(tries)}) として表すことができる。ここで、

clear は、クライアント 10 又はユーザに応じた数又はデータ (乱数との排他的論理和 (XOR) がとられたクライアント識別番号、又はユーザ識別番号若しくはユーザ加入番号など) である。

【0027】

K_{start} は、鍵サーチの始点として用いるための鍵である。

【0028】

{clear}_{K=H(tries)} は、試行の (すなわち、正しい鍵を求めるのに必要な反復の数の) ハッシュ値に対応する鍵によって暗号化された clear である。乱数との排他的論理和 (XOR) がとられた試行の数のハッシュ値に対応する鍵 K を用いることも可能である。

【0029】

別の好ましい実施例の鍵サーチ・アルゴリズムでは、

1. 試行カウンタ $i=1$ を初期化する

2. $K_i = K_{start} + i$ を計算する

3. $\{clear\}_{K_i}$ を計算する

4. 結果が $\{clear\}_{H(tries)}$ に等しいか否かを確認する

5a. 肯定の場合、暗号チャレンジCが破られた結果として K_i 及び試行数 i を検証器 20 に送出する

5b. 否定の場合、 i を増やし、工程 2 に進む。

【0030】

更に別の好ましい実施例では、暗号チャレンジCは、 $(clear, K_{start}, \{clear\}_{K=H(tries(K_{start}))})$ として表すことができる。ここで、

$clear$ は、クライアント 10 又はユーザに応じた数又はデータ（乱数との排他的論理和（XOR）がとられたクライアント識別番号、又はユーザ識別番号若しくはユーザ加入番号など）である。

【0031】

K_{start} は、鍵サーチの始点として用いるための鍵である。

【0032】

$\{clear\}_{K=H(tries(K_{start}))}$ は、 K_{start} を $tries$ 回ハッシングすることによって算出される値に対応する鍵によって暗号化された $clear$ である。

【0033】

別の好ましい実施例の鍵サーチ・アルゴリズムは、

1. $i=1$ 及び $K_0 = K_{start}$ に初期化する

2. $K_i = H(K_{i-1})$ を計算する

3. $\{clear\}_{K_i}$ を計算する

4. 結果が $\{clear\}_{H(tries(K_{start}))}$ に等しいか否かを確認する

5a. 肯定の場合、暗号チャレンジCが破られた結果として K_i 及び試行数 i を検証器 20 に送出する

5b. 否定の場合、 i を増やし、工程 2 に進む。

【0034】

更に別の実施例では、暗号チャレンジは、クライアント 10 がハッシュ関数を逆にすることを必要とする。

【0035】

クライアント 10 から結果 212 を受信すると、検証器 20 はそのタイマ 22 を停止させる（214）。すなわち、検証器のタイマは、チャレンジの送出と応答の受信との間の時間を測定する。検証器 20 は次いで、結果（すなわち、 $start+i$ ）が期待値（すなわち、 $start+tries$ ）に等しいこと（すなわち、 i が $tries$ に等しいこと）を確認する（216）。

【0036】

確認 216 が首尾良く行われなかった場合、検証器 20 は、クライアント 10 がエミュレートされていることが分かる。しかし、確認 216 が首尾良く行われた場合、検証器 20 は、そのタイマ 22 から読み出された値が、選ばれたネットワーク送信遅延を期待時間に加えたものを超えないことの確認（218）に進む。すなわち、検証器 20 は、応答 212 がタイムリーであることを確認する。それによって、適切な応答をハッカーが破るのに利用可能な時間が削減される。この第 2 の確認 218 が首尾良く行われた場合、クライアント 10 が期待プラットフォーム上で実行することを検証器 20 は結論付け得る。

【0037】

別の実施例では、検証器 20 は、期待プラットフォーム上で実行することを結論付ける前に、連続したいくつかのチャレンジにクライアント 10 が正しく応答することを必要とし得る。

10

20

30

40

50

【0038】

好ましい実施例では、クライアント10又はユーザにリンクした識別子やその他のデータ（例えば、排他的論理和（XOR）、加算、ハッシング又は暗号化によって乱数と組み合わせられたクライアント識別番号、又はユーザ識別番号若しくはユーザ加入番号など）である。これによって、ハッカーが、例えば2つのクライアント（すなわち、盗んだIDによってエミュレートされた一クライアント、及びエミュレートされていない一クライアント）を用いて、それらの一方に対する第1の検証工程及び他方に対する第2の工程を通過させることがより難しくなる。

【0039】

暗号チャレンジを識別子に依存させるために、サーバは好ましくは、start+triesの代わりにstart+tries+（識別子mod 2^{32} ）を用いて前述のチャレンジを作成する。サーバは次いで、結果を算出するが、start+triesのみをクライアントに送出する。それは、その識別子mod 2^{32} によってこれを完了する。よって、チャレンジが、エミュレートされていないプラットフォームに対して、正しい識別子を用いて行われたことが検証される。

【0040】

本発明は、暗号チャレンジの使用に限定されないが、クライアントが所定の手法によって算出を行い、必要な反復数を戻すことを必要とする他の種類のチャレンジを用いることもできる。例えば、特定の開始値から始まる、数学的関数の特定の精度までの反復的算出。

【0041】

本発明によって、ハッカーにとって一層難しくなるように適合させることができる、エミュレートされたクライアントの費用効果の高い検出が可能になる。

【0042】

本発明は例として説明しているに過ぎず、詳細の修正は、本発明の範囲から逸脱することなく行うことが可能である。

本明細書、並びに（該当する場合）特許請求の範囲、及び添付図面に記載された各構成は、別個に備えても、何れの適切な組み合わせで備えてもよい。ハードウェアで実現されるものとして記載した構成は、ソフトウェアによっても実現することができ、逆も同様である。接続は適宜、無線接続又は有線接続（必ずしも直接又は専用でなくてよい）として実現することができる。

【0043】

特許請求の範囲記載の参照符号は、例証の目的に過ぎず、特許請求の範囲記載の範囲を限定する効果を何ら有しないものとする。

【図面の簡単な説明】

【0044】

【図1】本発明の好ましい実施例によるクライアント及び検証器を示す図である。

【図2】本発明の好ましい実施例による、特定のプラットフォーム上でクライアントが実行することを検証する方法を示す図である。

【符号の説明】

【0045】

- 1 ネットワーク
- 10 クライアント
- 11 CPU
- 13 メモリ
- 14 I/O
- 20 検証器
- 21 CPU
- 22 タイマ
- 23 メモリ
- 24 I/O

10

20

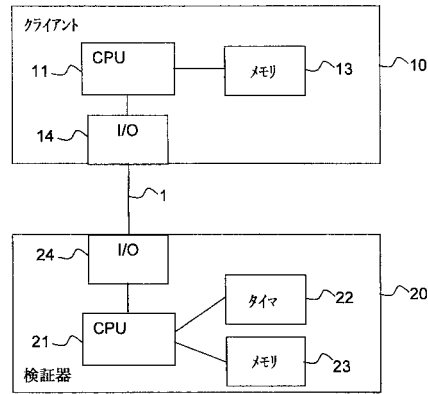
30

40

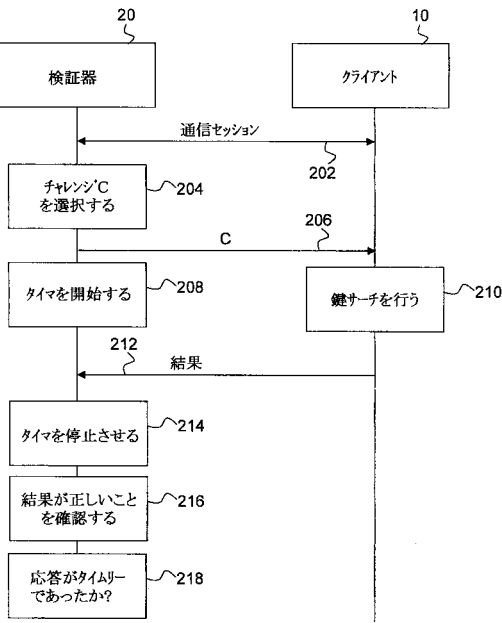
50

202 通信セッション
206 チャレンジ
212 結果

【図 1】



【図 2】



フロントページの続き

- (72)発明者 オリヴィエ イーン
フランス国, 3 5 4 1 0 ドンルー, リュ・デ・トゥルヌソル 2 0
- (72)発明者 エリック ディエル
フランス国, 3 5 3 4 0 リフレ, ラ・ビュザールディエール (番地なし)
- (72)発明者 アラン デュラン
フランス国, 3 5 0 0 0 レヌヌ, リュ・ド・ディナン 7 9
- (72)発明者 モハメッド カルミ
フランス国, 3 5 2 0 0 レヌヌ, リュ・デュ・グヴェルヌール・ジェネラル・フェリックス・エ
ブエ 8
- (72)発明者 ニコラ プリジャン
フランス国, 3 5 0 0 0 レヌヌ, リュ・アンリ・ル・ギュー 3 1
- Fターム(参考) 5B285 AA01 BA02 CA41 CA47
5J104 AA07 KA01 KA04 KA06 PA07 PA16