

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号
特許第4988846号
(P4988846)

(45) 発行日 平成24年8月1日(2012.8.1)

(24) 登録日 平成24年5月11日(2012.5.11)

(51) Int.Cl.

F I

HO 4 L 9/32 (2006.01)

HO 4 L 9/14 (2006.01)

HO 4 L 9/08 (2006.01)

HO 4 L 9/00 6 7 5 A

HO 4 L 9/00 6 4 1

HO 4 L 9/00 6 0 1 C

請求項の数 4 (全 5 頁)

(21) 出願番号	特願2009-525007 (P2009-525007)	(73) 特許権者	507189219
(86) (22) 出願日	平成19年8月7日 (2007.8.7)		ノキア シーメンス ネットワークス ゲ
(65) 公表番号	特表2010-502068 (P2010-502068A)		ゼルシャフト ミット ベシュレンクテル
(43) 公表日	平成22年1月21日 (2010.1.21)		ハフツング ウント コンパニー コマ
(86) 国際出願番号	PCT/EP2007/058203		ンディトゲゼルシャフト
(87) 国際公開番号	W02008/022917		Nokia Siemens Netwo
(87) 国際公開日	平成20年2月28日 (2008.2.28)		rks GmbH & Co. KG
審査請求日	平成21年3月23日 (2009.3.23)		ドイツ連邦共和国 ミュンヘン ザンクト
(31) 優先権主張番号	102006039327.9		マルティン シュトラーセ 76
(32) 優先日	平成18年8月22日 (2006.8.22)		St. Martin Str. 76,
(33) 優先権主張国	ドイツ (DE)		D-81541 Muenchen,
			Germany
		(74) 代理人	100061815
			弁理士 矢野 敏雄

最終頁に続く

(54) 【発明の名称】 認証方法

(57) 【特許請求の範囲】

【請求項 1】

サーバに対してクライアントを認証する方法において、

a) 前記のクライアントおよびサーバにより、同じアルゴリズムにしたがいかつ互いに依存せずに第1キー（イプシロンキー）を形成し、ここで前記のアルゴリズムおよび当該のアルゴリズムのスタートキーは、クライアントとサーバとの間の秘密の取り決めにて前もって決定されており、

b) 前記のクライアントによって第2キーを形成して、当該第2キーと第1キーとの間の間隔（デルタ）があらかじめ定めた間隔内にあるようにし、ここで前記の複数のキーのメトリックは秘密の取り決めによってクライアントとサーバとの間で前もって決定されており、

c) 前記の第2キーをサーバに送信し、

d) 前記の受信した第2キーと第1キーとの間隔が、あらかじめ定めたデルタ内にある場合には前記のクライアントがサーバによって正当であると認証され、

e) 前記のクライアントがサーバによって正当であると認証された場合、サーバに対するクライアントの後続の認証のための新たなスタートキーとして前記の第2キーを使用することを特徴とする、

サーバに対してクライアントを認証する方法。

【請求項 2】

キーとして2進数を使用する、

請求項 1 に記載の方法。

【請求項 3】

前記の 2 つのキーの間隔（デルタ）として 2 つの 2 進数の差分を使用する、
請求項 2 に記載の方法。

【請求項 4】

前記のアルゴリズムを L F S R によって実現する、
請求項 1 から 3 までのいずれか 1 項に記載の方法。

【発明の詳細な説明】

【技術分野】

【0001】

10

本発明の根底にある問題

本発明の根底にある問題は、パスワードをクリアテキストで伝送することなく、クライアントをサーバにおいて認証することである。つねに同じキーで符号化されるパスワードではインターセプトされて、正当でない人に使用される可能性がある。

【0002】

上記の問題に対するこれまでの解決手段

従来の方法では、サーバによってランダムに発生させて符号化しかつ署名したチャレンジテキスト（署名済みチャレンジ）が、クライアントによって要求されて送られる。クライアントは、これを復号化し、ダイジェストを形成して署名し、再びこれを符号化する（署名済みダイジェスト）。サーバは、このダイジェストが一致するか否かを検査する。この方法は極めて繁雑である。

20

【0003】

上記の問題に対して考えられ得る別の解決手段

上記の最初の認証の前に T A N リスト（オンラインパッド）と類似に別の経路（例えば紙）で複数の鍵（キー）を有する（有限の）リストを交換し、これらのキーをそれぞれ一度だけすることもできる。しかしながらこのリストは、記憶するかまたはユーザはこれらのキーを書き写さなければならない（攻撃可能である、ないしは場合によって誤りを犯しやすい）。

【0004】

上記の問題に対する本発明の解決手段

30

以下では 1 つの図を含む図面に用いて本発明を詳しく説明する。

【図面の簡単な説明】

【0005】

【図 1】本発明の認証方法を説明する図である。

【0006】

両側（クライアントおよびサーバ）は、最初に鍵（キー）を生成するため、（シードの一部として）同じスタート値および同じアルゴリズムとを取り決める。

【0007】

これにより、クライアントおよびサーバは、互いに無関係にキーの同じシーケンスを形成することができる。このようにして生成され得るシーケンスを P R B S（Pseudo Random Binary Sequence）とも称する。P R B S の生成は、例えば、L F S R（Linear Feedback Shift Register）を用いて実現することができる。

40

【0008】

しかしながら P R B S は、厳格に決定的（streng deterministisch）である。したがってわずかな個数の結果（キー）にしたがって上記の方法を求めることができ、この場合に攻撃者に別のすべてのキーがわかってしまうのである。さらに有限個のキーの後、キー列の精確な繰り返しが発生してしまうのである（L F S R の周期性）。

【0009】

しかしながら上記の流れ（すなわち L F S R を用いたキーの生成）に規則的な間隔で障害（Stoerungen）を挿入すると、結果は周期的でも決定的でもなくなるのである。

50

【0010】

上記の流れにおける障害はつぎのように達成される（これについて図も参照されたい）。

【0011】

まずクライアントおよびサーバは、上記のスタート値（スタートキー）からLFSRを用いて第1キーを生成する。区別し易くするため以下ではこれをイプシロンキー ϵ と称する。このイプシロンキーは、攻撃が可能であるため、認証には使用しない。

【0012】

つぎにクライアントだけが第2キーを生成し、をクライアントはこのキーサーバに送信する。この第2キーだけを上記の認証に使用する。LFSRを用いた生成とは異なる第2キーの生成を理解するため、メトリック（Metrik）に小さな補足を行う。

【0013】

補足：

メトリックとは、2つの点の間隔（デルタ）の定め方のことである。コンピュータによってビットで記憶される数に適用した場合、最も簡単なケースではこれは2つの数の差分のことである。2つの2進数の差分は、2つの数の個々のビットの重み付け（Wertigkeit）に依存する。ふつうビットの重み付けは、0（ 2^0 ）から31（ 2^{31} ）の伝送順序によって決まる（従来のメトリック）。すなわち、

【表1】

従来のメトリック： 31.....6543210

```
-----
2503657302 ( 10010101001110101100011101010110 )
+ 536936480 ( 001000000000000010000000000100000 )
= 3040593782 ( 10110101001110111100011101110110 )
-----
```

新しいメトリック： 1 0 2

である。

【0014】

数3040593782と数2503657302との間隔は、従来のメトリックによれば、536936480である。ここで種々異なるビットに対して新しい重み付けを設定ないしは取り決めて新たなメトリックを定めると、上記の2つの数は異なる間隔を有する。例えば、ビット16がビット0（ 2^0 ）の新しいビット重み付けを、ビット29がビット1（ 2^1 ）の新しいビット重み付けを、またビット5がビット2（ 2^2 ）の新たなビット重み付けを得ると、上記の2つの数は、単に間隔7を有することになる。別のビットの順序は、これに対して重要ではないが、これらのビットの状態（0または1）は重要である。7までのデルタを考察すると、新たなメトリックによれば、数3040593782は、2503657302のこのデルタ内に存在し、これに対して2503657303は、2503657302から7よりも離れている。それは、2よりも大きな重み付けを有する1ビットが異なるからである。

【0015】

本発明では、伝送順序とは異なる別の重み付けを有するビット（いわゆる障害ビット）が設定されることにより、（シードの一部として）クライアントとサーバとの間で新たなメトリックについての取り決めが行われるのである。

【0016】

3040593782を上記のクライアントおよびサーバによって生成した第1キー（イプシロンキー）とする。この場合に次キー（第2キー）として、クライアントにより、つぎのようなキーを形成する。すなわち、その間隔（デルタ）が、上記の新たなメトリックによれば、上記のイプシロンキーに対してあらかじめ定めた値内にあるようなキーを形成するのである。このキーを以下では、デルタキー δ と称する。すなわち、上記のクライアントが、

次キーとして数478651654を形成する場合、これはデルタキーである。それは、この数が上記のイプシロンキーのデルタ内にあるからである。

【0017】

上記のクライアントおよびサーバだけが、障害ビットの位置によって変化した新しいメトリックを知っているため、サーバは上記のクライアントを上記の受信した第2キーに基づいて認証することができる。上記のクライアントによって送信された第2キーが、上記のデルタ内にある場合、このクライアントは認証される。両側においてこのキーが、新たなシードとして使用され、LFSRにおけるさらなるシフトが、新たな第1キー（新たなイプシロンキー）になるのである。

【0018】

10

上記の例では、32ビットだけを示した。実際には上記の数はさらに格段に大きく、すなわち例えば8個または16個の障害ビットを有する2048または4096ビットである。上記の間隔を求めるのに差分とは別の演算を使用することも可能である。

【0019】

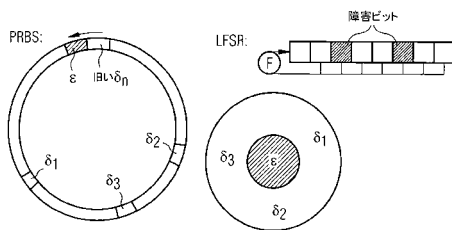
n を障害ビットの数とすると、 $2^n - 1$ 個のすべてのデルタキーは、上記のデルタ、すなわち、既知のメトリックのイプシロンの周囲値（Umgebung）を形成する。この周囲値そのものは、障害ビットの位置によって両側に既知であり、かつ攻撃者が求めることができないからである。

【0020】

上記の新しい解決手段の利点はずぎの通りである。すなわち、最初のシードの一部として一度、スタートキーを従来の方式で交換しなければならないが、その後は、新たなメッセージ毎に新たなデルタから得られるキーだけを送ればよいのである。

20

【図1】



フロントページの続き

- (74)代理人 100094798
弁理士 山崎 利臣
- (74)代理人 100099483
弁理士 久野 琢也
- (74)代理人 100112793
弁理士 高橋 佳大
- (74)代理人 100128679
弁理士 星 公弘
- (74)代理人 100135633
弁理士 二宮 浩康
- (74)代理人 100114890
弁理士 アインゼル・フェリックス＝ラインハルト
- (72)発明者 マティーアス ヘーネ
ドイツ連邦共和国 ランゲヴァール シュトライトベルガー シュトラーセ 27

審査官 青木 重徳

- (56)参考文献 特開2002-217884 (JP, A)
国際公開第2006/003711 (WO, A1)
国際公開第02/91668 (WO, A2)
国際公開第00/79457 (WO, A1)
米国特許第5148007 (US, A)

- (58)調査した分野(Int.Cl., DB名)
H04L 9/32
H04L 9/08
H04L 9/14