(19) Deutsches Patent- und Markenamt

(10) **DE 10 2009 007 277 A1** 2010.08.05

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2009 007 277.2**
(22) Anmeldetag: **03.02.2009**
(43) Offenlegungstag: **05.08.2010**

(51) Int Cl.[8]: ***H04L 9/28*** (2006.01)
H04L 9/32 (2006.01)

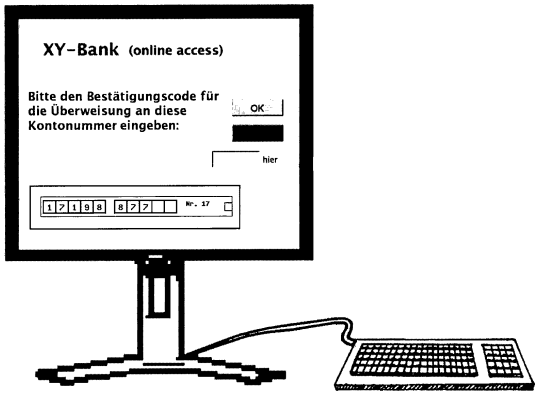
(71) Anmelder:
Borchert, Bernd, Dr., 48480 Lünne, DE

(72) Erfinder:
gleich Anmelder

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Fälschungssichere Online Transaktionen**

(57) Zusammenfassung: Die vorliegende Erfindung betrifft ein Verfahren zur manipulationssicheren Verschlüsselung für Online-Accounts, insbesondere für Online-Banking, mittels Bildern von mit Zeichen der Transaktion beschrifteten Flächen. Der Account-Benutzer ist in der Lage, Transaktionendaten manipulationssicher zu übermitteln.



Beschreibung

[0001] Die vorliegende Erfindung betrifft ein Verfahren zur manipulationssicheren Verschlüsselung für Online-Accounts, insbesondere für Online-Bankkonten.

[0002] Die Abhör- und Manipulations-Sicherheit von Online-Accounts – insbesondere die von Online-Bankkonten – wird durch die immer größer werdende Quantität und Schädlichkeit von Malware (d. h. Viren etc.) auf den PC's der Bankkunden gefährdet. Verfahren, die das Abhören der PIN und/oder einen sogenannten Man-in-the-Middle Fälschungs-Angriff sicher verhindern, sind technisch aufwändig und benötigen spezielle Hard- und Software auf dem vom Bankkunden benutzten PC.

[0003] Der sogenannte Man-in-the-Middle Fälschungs-Angriff auf eine mit dem TAN oder iTAN Verfahren abgesicherte Überweisung verläuft folgendermaßen: Bankkunde X möchte 50 Euro auf das Konto von Y überweisen. Er füllt das entsprechende Online Formular aus und schickt es ab. Die Malware auf dem Rechner fängt diesen Überweisungsauftrag ab, bevor er an die Bank geschickt wird, wandelt ihn in eine Überweisung von 5000 Euro an Z um, und schickt diesen manipulierten Überweisungsauftrag an die Bank. Die Nachfrage der Bank an X nach einer iTAN für den Überweisungsauftrag von 5000 Euro an Z wird von der Malware in der umgekehrten Richtung ebenfalls abgefangen, und es wird dem Bankkunden X am Bildschirm die Nachfrage der Bank nach einer iTAN für einen Überweisungsauftrag von 50 Euro an Y vorgespiegelt. Ahnungslos bestätigt X mit einer TAN diesen vorgespiegelten Auftrag, und die Malware schickt die von X eingegebene iTAN an die Bank weiter, um den betrügerischen Überweisungsauftrag von 5000 Euro an Z zu bestätigen.

[0004] Die Verfahren PIN/TAN, PIN/iTAN, HBCI-1, HBCI-2, und Security Token schützen nicht sicher vor dem Man-in-the-Middle Angriff. Auch die Verschlüsselung der Verbindung (z. B. SSL) schützt nicht sicher, denn die Malware kann sich schon vor Beginn der Verbindungs-Verschlüsselung einschalten und die Manipulationen noch vor der Verbindungs-Verschlüsselung (bzw. in der anderen Richtung: nach der Verbindungs-Entschlüsselung) durchführen.

[0005] Beispiele von Verfahren, die sicher vor dem Man-in-the-Middle-Angriff schützen, sind die, die eine Anzeige außerhalb des Klienten Rechners anbringen, wie z. B. HBCI-3. Allerdings besteht wegen der physikalisch bestehenden Kabelverbindung zwischen dieser Extra-Hardware und dem Rechner des Klienten immer noch ein Restrisiko, dass Malware auf dem Rechner des Klienten die Aktionen auf der Extra-Hardware ausspioniert.

[0006] Eine weitere Möglichkeit ist es, sich die Überweisungsdaten per SMS von der Bank bestätigen zu lassen („mTANs”). Nachteilig an dieser Lösung ist, dass ein Handy vorhanden sein muss und dass der Empfang der SMS eventuell eine Weile dauert. In Funklöchern und im Ausland funktioniert das System nicht. Außerdem ist es nur eine Frage der Zeit, bis auch Handys von Malware befallen werden und damit diese Möglichkeit auch unsicher wird.

[0007] Die Patente EP1472584B1, US2005/0219149A1 und DE-10-2007-018802.3, 2007 schlagen vor, die Sicherheit von Online Accounts mittels Visueller Kryptographie zu gewährleisten.

[0008] Das Patent WO-2006-020096 und die Patentanmeldung DE-10-2007-029759.0 schlagen vor, die Sicherheit von Online Accounts mittels Cardano Kryptographie zu gewährleisten.

[0009] Die Patentanmeldung DE-10-2007-029759.0 schlägt vor, die Sicherheit von Online Accounts mittels eines elektronischen Geräts mit Fotosensoren und Display zu gewährleisten.

[0010] Die Aufgabe der vorliegenden Erfindung ist es, ein sicheres Verschlüsselungsverfahren für Online-Accounts bereit zu stellen, das das Übermitteln einer nicht manipulierbaren Nachricht, z. B. die Zielkontonummer einer Überweisung, vom Klienten an den Server erlaubt.

[0011] Das Patent WO02/17556A1 schlägt vor, mithilfe von ausgedruckten Linien-Permutationen die Authentifizierung zu Online Accounts sicherer zu machen, in dem Sinne, dass man, um Zugang zum Account zu erhalten, die ausgedruckte Linien-Permutation haben muss und das Passwort kennen muss, wobei das Passwort nicht abhoerbar ist. Es wird mit dem in dem Patent beschriebenen Verfahren nur die Authentifizierung abgesichert, aber es wird kein Schutz vor Fälschung von Transaktionen – wie zum Beispiel Überweisungen – geboten.

[0012] Die vorliegende Erfindung stellt ein weiteres low-tech Verfahren zur manipulationssicheren Übertragung von Transaktionsdaten bei Online Accounts vor.

[0013] Zu diesem Zweck werden die vom Account-Server beschriftete Flächen nach dem Zufallsprinzip erzeugt, und ebenso zufällig erzeugte Zeichenreihen (TAN). Dann werde sie nummeriert, gespeichert, gedruckt und dem Account-Benutzer auf einem möglichst sicherem Weg zugesandt.

[0014] Für eine Transaktion tippt der Account-Benutzer die Transaktionsdaten am Bildschirm ein. Zur Bestätigung der Transaktion fragt der Account-Ser-

ver am Bildschirm nach einem bestimmten Bild mit beschrifteten Flächen, z. B. unter Angabe einer Nummer, und zeigt die Transaktionsdaten am Bildschirm ebenfalls als Bild mit beschrifteten Flächen an, die ähnlich angeordnet sind.

[0015] Jetzt kann ein Code-Wort eingegeben werden: für jeden Buchstaben der TAN sucht der Benutzer die Positionen, in denen der Buchstabe vorkommt und gibt als Code den Buchstaben ein, der auf der Papier-Leiste auf der entsprechenden Fläche steht.

[0016] Das Verfahren verhindert das Fälschen der Transaktion durch einen Trojaner, denn wenn der Trojaner andere, d. h. gefälschte, Transaktionsdaten zum Account-Server schickt, dann gibt der Account-Benutzer zur Bestätigung ein Codewort ein, das mit höchster Wahrscheinlichkeit ein anderes ist als der Account-Server erwartet: deshalb wird dann die gefälschte Transaktion als nicht bestätigt angesehen und nicht ausgeführt.

[0017] Weil die Malware (auf dem Rechner des Bankkunden oder im Rechnernetz) die zufällig erzeugten Bilder mit den Flächen und auch die TANs nicht kennt und definitiv auch nicht ausspionieren kann, und gleichzeitig die Buchstaben, die die Transaktion beschreiben, auch zur Bestätigung herangezogen werden, stellt das Verfahren einen effektiven Schutz gegen Fälschung dar.

[0018] In der Zeichnung zeigt:

[0019] In Abb. 1 wird die Situation beim Online Banking gezeigt: der Kunde gibt die Code-Buchstaben für die TAN nacheinander ein, jeweils in der Kontonummer von links nach rechts suchend.

Ausführungsbeispiel

[0020] Das oben angegebene Verfahren zur Sicherung einer Nachricht gegen Fälschung wird angewandt auf den speziellen Fall des Online-Bankings. Das Verfahren verhindert den Man-in-the-Middle Fälschungs-Angriff auf die Daten einer Überweisung.

[0021] Der Bank-Server erzeugt für den Bankkunden X eine Menge von Leisten von Flächen mit zufällig gewählten Buchstaben (es werden keine Ziffern genommen, um den Bankunden nicht zu verwirren) und jeweils dazu eine 6-stelligen TAN, nummeriert sie, speichert sie ab, druckt sie auf Papier aus und schickt sie dem Bankkunden per Post zu (also so ähnlich wie TAN-Listen verschickt werden).

[0022] Wenn der Kunde X die Leisten empfangen hat, kann er mit dem Online Banking beginnen. Der Kunde loggt sich ein (wie üblich mit einer PIN) und geht auf ein Überweisungsformular. Er trägt in das Formular die Überweisungsdaten ein und schickt das Formular zum Bank-Server. Der Bank-Server schickt zur Bestätigung die Überweisungsdaten auf den Bildschirm des Kunden. Dabei hat die Kontonummer eine besondere Bedeutung: Sie wird ebenfalls als Leiste von beschrifteten Flächen dargestellt. Die Situation ist in Abb. 1A dargestellt.

[0023] Der Kunde knickt sein Papier so, dass er genau die Leiste mit der nachgefragten Nummer an den Bildschirm unter die dort dargestellte Leiste mit der Kontonummer halten kann.

[0024] Jetzt kann der Kunde das Codewort zur Bestätigung, das in dem Fall aus Buchstaben besteht, eingeben: für die TAN mit dieser Nummer geht er sukzessive deren Ziffern durch und sucht für jede dieser Ziffer die Positionen der Kontonummer, die diese Ziffer haben. Für diese Position gibt er den Buchstabencode ein, der auf der druntergehaltenen Leiste auf dem Papier zu sehen ist.

[0025] Auf diese Art gibt der Bankkunde sukzessive einen Bestätigungscode aus Buchstaben ein. Der Code wird zur Bank geschickt. Die Bank kann prüfen, ob der Kunde den Bestätigungscode richtig eingegeben. In dem Fall wird die Überweisung ausgeführt.

[0026] Das Verfahren sichert die Überweisung gegen Fälschung ab: wenn der Trojaner andere Transaktionsdaten zum Bank-Server schickt als auf dem Bildschirm dargestellt werden, wird mit hoher Wahrscheinlichkeit vom Bankkunden ein Codewort eingegeben, das der Bank-Server als falsch ansehen wird. Das passiert mit einer gewissen Wahrscheinlichkeit auch schon dann, wenn auch nur eine Ziffer vom Trojaner verändert wird.

ZITATE ENTHALTEN IN DER BESCHREIBUNG

Diese Liste der vom Anmelder aufgeführten Dokumente wurde automatisiert erzeugt und ist ausschließlich zur besseren Information des Lesers aufgenommen. Die Liste ist nicht Bestandteil der deutschen Patent- bzw. Gebrauchsmusteranmeldung. Das DPMA übernimmt keinerlei Haftung für etwaige Fehler oder Auslassungen.

Zitierte Patentliteratur

- EP 1472584 B1 **[0007]**
- US 2005/0219149 A1 **[0007]**
- DE 10-2007-018802 **[0007]**
- WO 2006-020096 **[0008]**
- DE 10-2007-029759 **[0008, 0009]**
- WO 02/17556 A1 **[0011]**

Patentansprüche

1. Verfahren zur manipulationssicheren Übertragung einer Zeichenreihe x bestehend aus Zeichen eines Alphabets A von einem Klienten durch ein Rechnernetz zum Server, gekennzeichnet durch die folgenden Schritte:
a) das Erzeugen eines Bildes mit Flächen, die nach dem Zufallsprinzip mit Zeichenreihen eines weiteren Alphabets B beschriftet werden, durch den Server,
b) das Erzeugen eine Zeichenreihe y bestehend aus Zeichen des Alphabets A durch den Server,
c) die Zustellung des in a) erzeugten Bildes mit Flächen und der in b) erzeugten Zeichenreihe an den Klienten,
d) die Darstellung der zu übertragenden Zeichenreihe x auf dem Bildschirm des Klienten auf mit Zeichen aus A beschrifteten Flächen, die ähnlich angeordnet sind wie die in a) erzeugten Flächen,
e) die Eingabe einer Reihe von Zeichen aus dem Alphabet B durch den Klienten, indem dieser für jedes der in der Zeichenreihe y vorkommenden Zeichen i Beschriftungen der Flächen auf dem ihm zugestellten Bild auswählt und eingibt, die den auf dem Bildschirm dargestellten, mit dem Zeichen i beschrifteten Flächen durch ihre analoge Lage entsprechen,
f) die Übertragung dieser Zeichenreihe zum Server,
g) die Prüfung der vom Klienten eingegebenen Zeichenreihe durch den Server.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Alphabete A und B gleich, sind, oder eins ein Teilalphabet des anderen ist, oder A und B unvergleichbar sind oder beide sogar keine gemeinsamen Elemente haben.

3. Verfahren nach einem der vorgehenden Ansprüche, dadurch gekennzeichnet, dass das Alphabet A aus den Ziffern 0,...,9 besteht,

4. Verfahren nach einem der vorgehenden Ansprüche, dadurch gekennzeichnet, dass die in 1) a) erzeugten Zeichenreihen nur aus einem oder aus maximal einem Zeichen bestehen,

5. Verfahren nach einem der vorgehenden Ansprüche, dadurch gekennzeichnet, dass die in 1) b) erzeugte Zeichenreihe ein Passwort oder eine PIN ist und sich bei einer Wiederholung des Verfahrens nicht ändert,

6. Verfahren nach einem der vorgehenden Ansprüche, dadurch gekennzeichnet, dass die Reihenfolge der Verarbeitung der Zeichen i in 1) e) der Reihenfolge der Zeichen in der Zeichenkette y entspricht,

7. Verfahren nach einem der vorgehenden Ansprüche, dadurch gekennzeichnet, dass die in 1) e) ausgewählten Flächen alle solchen Flächen sind oder nur eine bestimmte Teilmenge sind, und die Reihenfolge der Auswahl eine vorgegebene ist oder beliebig ist,

8. Verfahren nach einem der vorgehenden Ansprüche, dadurch gekennzeichnet, dass das erzeugte Bild und die Zeichenreihe auf Papier ausgedruckt wird und dem Klienten zugestellt wird.

9. Verfahren nach einem der vorgehenden Ansprüche, dadurch gekennzeichnet, dass das erzeugte Bild und die Zeichenreihe auf durchsichtige Folie oder auf durchsichtiges Papier ausgedruckt wird und dem Klienten zugestellt wird.

10. Verfahren nach einem der vorgehenden Ansprüche, dadurch gekennzeichnet, dass mehrere erzeugte Bilder und Zeichenreihe auf das gleiche Blatt Papier oder die gleiche Folie ausgedruckt werden und mit eindeutigen Namen oder Nummern versehen dem Klienten zugestellt werden.

11. Verfahren nach einem der vorgehenden Ansprüche, dadurch gekennzeichnet, dass das erzeugte Bild und die Zeichenreihe per SMS oder anderer elektronischer Datenübertragung dem Klienten zugestellt wird.

12. Verfahren nach einem der vorgehenden Ansprüche, dadurch gekennzeichnet, dass das erzeugte Bild via Display eines elektronischen Security Tokens dem Klienten zugestellt wird. Das Security Token wird dabei als Teil des Servers angesehen.

13. Vorrichtung nach einem der vorgehenden Ansprüche, gekennzeichnet dadurch, dass die Bilder mit den beschrifteten Flächen elektronisch auf ihr gespeichert sind.

14. Vorrichtung nach einem der vorgehenden Ansprüche, gekennzeichnet dadurch, dass die dargestellten Bilder und Zeichenreihen mit den beschrifteten Flächen per SMS oder anderer elektronischer Datenübertragung empfangen werden.

15. Computerprogrammprodukt, vorgesehen dafür zu sorgen, dass ein Prozessor das Verfahren nach einem der Ansprüche 1 bis 14 durchführt.

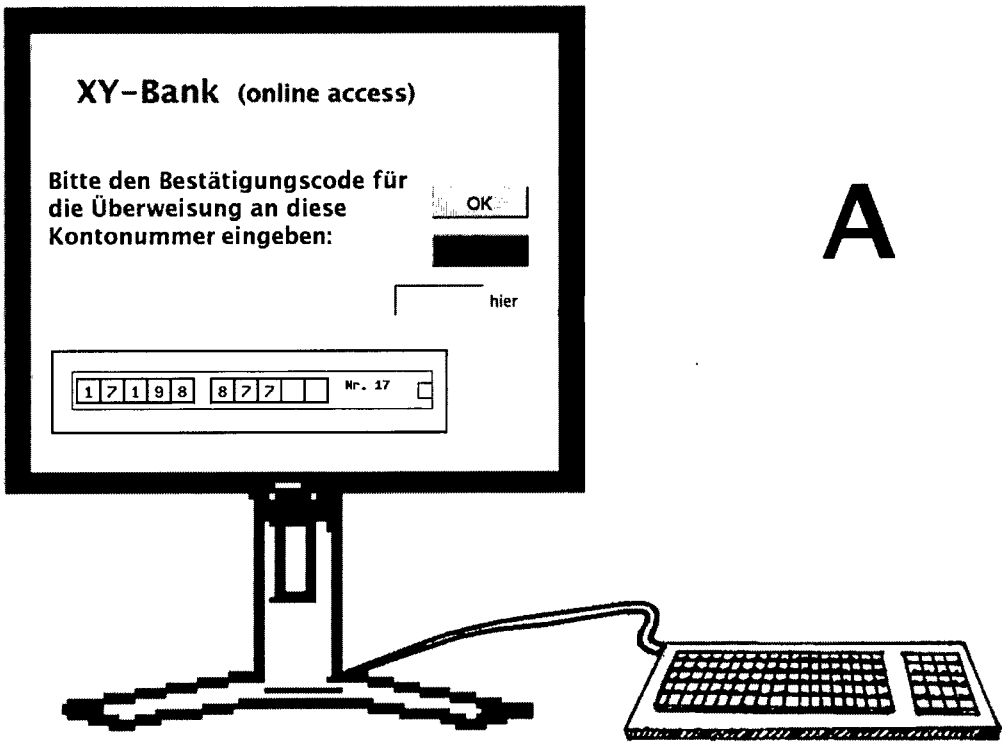
16. Server vorgesehen dafür zu sorgen, dass ein Prozessor das Verfahren nach einem der Ansprüche 1 bis 14 durchführt.

17. Verwendung des Verfahrens, des Computerprogrammprodukts, des Servers, der Vorrichtung oder des auf Folie oder Papier ausgedruckten Bildes und Zeichenreihe gemäß einem der vorgehenden Ansprüche bei Online-Accounts.

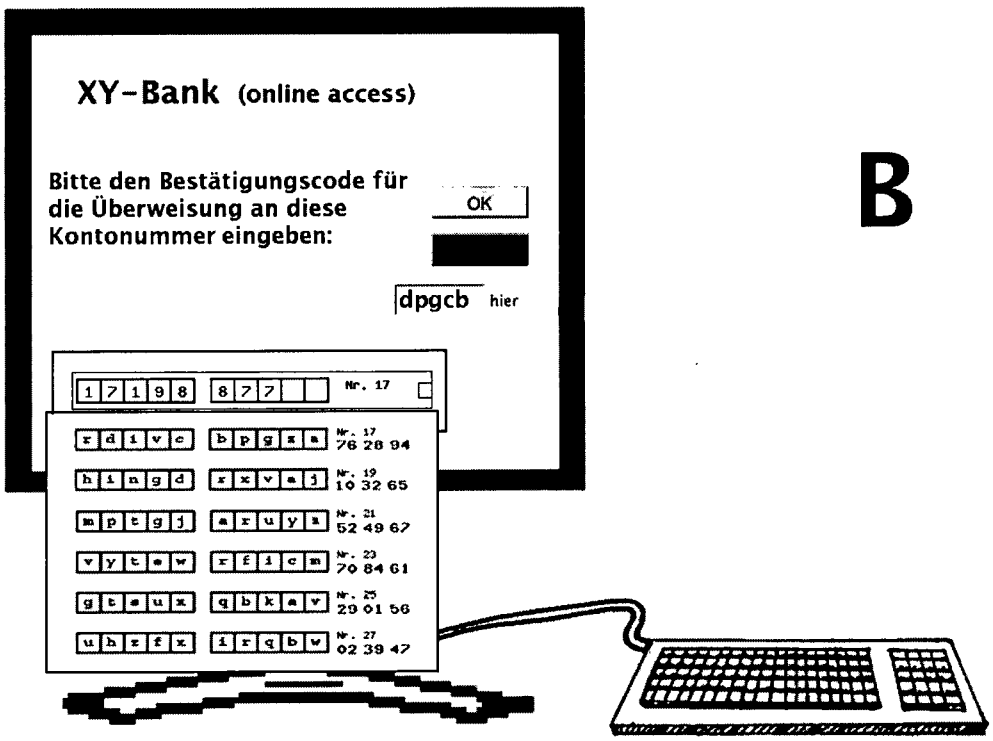
Es folgt ein Blatt Zeichnungen

Anhängende Zeichnungen

Bild 1



A



B