Kreativer Umgang mit IT-Sicherheitslücken – Absicherung von Online-Transaktionen mit VTANs*

Ulrich Greveler
Labor für IT-Sicherheit, Fachhochschule Münster
greveler@fh-muenster.de

07. Oktober 2007

Wir betrachten die Problemstellung, dass aufgrund von Sicherheitslücken bzw. fahrlässigem Nutzerverhalten *bösartige Software* (Malware) auf dem PC angenommen werden muss, dieser PC aber für finanzielle Transaktionen (*Online-Banking*) genutzt werden soll. Ist eine Lösung denkbar, die sichere Transaktionen ermöglicht, obwohl der PC nicht vertrauenswürdig ist? Wir beschreiben ein Verfahren, das die authentische Online-Übertragung von Transaktionen ermöglicht. Es verwendet visuelle Kryptographie anstelle von Transaktionsnummern (TANs), wie sie im Online-Banking-Bereich verbreitet sind.

1 Hintergrund

Die Abwicklung von Bankgeschäften vom häuslichen PC aus ist alltäglich geworden. *Electronic Banking* ist bequem für den Kunden und kostensparend für das Kreditinstitut. Die Übertragung sensibler Daten über ein öffentliches Netz birgt Sicherheitsrisiken (Mitschneiden bzw. Verändern der übertragenen Daten), denen durch Absicherung der Kommunikation (Authentifizierung, Verschlüsselung) entgegengewirkt wird.

In den letzen Jahren wurde vermehrt über Angriffe berichtet [5], die den Bankkunden im Visier haben und ihn dazu bringen sollen, geheime Autorisierungsdaten an die Angreifer herauszugeben (z. B. Phishing). Durch gezielte visuelle Täuschung mit technischen Mitteln (auch mit *Visual Spoofing* [1] bezeichnet) oder auch durch trickreich formulierte

*Der Beitrag stellt eine aktualisierte und auf eine breitere Zielgruppe zugeschnittene Version der Publikation *VTANs – Eine Anwendung visueller Kryptographie in der Online-Sicherheit* des Autors, vorgetragen auf dem *2. Workshop Kryptologie in Theorie und Praxis* (2007) in Bremen, erschienen in *Lecture Notes in Informatics* P-110 (ISBN 978-3-88579-204-8) dar.

E-Mails wird der Kunde über die Identität seines Kommunikationspartners getäuscht und zur Preisgabe seiner Zugangsdaten (geheime PIN und TANs) gebracht.

Darüber hinaus ist das Endgerät auf Kundenseite (der PC) Ziel von Attacken. Während die Kreditinstitute umfangreiche und aufwändige Maßnahmen zur Absicherung ihrer Systeme treffen, haben sie auf die kundenseitig eingesetzte Hard- und Software keinen oder nur geringen Einfluss, so dass Risiken aufgrund der Verbreitung von *Malware* bestehen [2].

Malware bezeichnet hier eine Software, die unbemerkt vom Benutzer auf seinem PC installiert wurde und dazu dient, ihm zu schaden (z. B. Daten auszuspionieren, die grafische Oberfläche fernzusteuern oder gezielt finanzielle Transaktionen zu manipulieren, so dass Geld unbemerkt auf fremde Konten überwiesen wird). Eine solche Malware kann über die Verbreitung von Viren, Programmen mit Hintertüren (*Trojanische Pferde*) oder allgemeine Sicherheitslücken des Betriebssystems oder einer Anwendungssoftware (durch sogenannte Hackerangriffe) auf den PC gelangt sein.

2 Angreifermodell

Die Rolle einer Person oder eines Programmes, die beabsichtigen, bestehende Sicherheitsanforderungen zu unterlaufen, wird allgemein als *Angreifer* bezeichnet. Zunächst legen wir die Fähigkeiten des Angreifers fest. Es gilt der Grundsatz: Je fähiger ein Angreifer ist, gegen den wir uns schützen können, desto besser müssen unsere Sicherheitsmaßnahmen sein.

In diesem Beitrag wird ein weitreichendes Angreifermodell zugrundegelegt. Der Angreifer, gegen den wir uns schützen wollen ist omnipotent: Der Angreifer

- kennt die eingesetzten Verfahren,
- kann den Kommunikationskanal (Internet) abhören und beliebig beeinflussen,
- hat unbeschränkte Rechenzeit und ausreichend kurze Reaktionszeiten,
- hat (über Malware) unbeschränkte Herrschaft über den PC des Kunden.

Das besondere Interesse des Angreifers liegt in Bezug auf die folgenden Überlegungen darin, seine Möglichkeiten zu nutzen, um finanzielle Transaktion, die via Online-Banking vorgenommen werden, zu manipulieren. Die übliche Absicherung über einen verschlüsselten und integritätsgesicherten Kanal (nach SSL-TLS-Standard[1]) ist hier nicht ausreichend, da die Malware Transaktionsdaten manipulieren kann, bevor diese die Banking-Applikation verlassen, ohne dass die visuelle Repräsentation auf dem Bildschirm (die Anzeige der Überweisungsdaten) verändert wird. Die Daten werden dann bereits verfälscht über den sicheren Kanal übertragen, so dass diese Absicherung nutzlos ist.

[1] SSL-TLS ist der kryptographische Standard, der angewandt wird, wenn der Nutzer im Browser als URL-Präfix `https` anstatt `http` verwendet und der Webserver dies unterstützt. Der Standard erlaubt neben einer Verschlüsselung die Sicherung der Nachrichten-Integrität und -Authentizität.

2.1 Online-Überweisung als schützenswerte Transaktion

Online-Banking erlaubt meist eine Reihe von Nutzeraktionen, die je nach Sichtweise des betroffenen Bankkunden einem unterschiedlichen Schutzbedarf unterliegen. Eine Abfrage des Kontostandes durch unberechtigte Dritte wird i. a. als erhebliche Datenschutzverletzung bewertet, so dass diese Operation nur nach erfolgreicher Authentifizierung ausgeführt werden kann. Als noch gravierender ist jedoch die (nicht autorisierte) Überweisung auf ein fremdes Konto zu bewerten, da der drohende finanzielle Verlust von den meisten Kunden als größte Gefahr des Online-Banking angesehen wird [7]. Wir konzentrieren uns daher in den folgenden Abschnitten auf die Absicherung der Überweisung, weisen aber darauf hin, dass das vorgestellte Verfahren für weitere Transaktionsarten, insbesondere auch für Kontostandsabfragen, verwendbar ist.

Die Transaktion, die wir schützen möchten, besteht aus einer Banküberweisung, die wir – um ein anschauliches Beispiel zu haben – folgendermaßen spezifieren:

```
Überweisung
von Konto-Nr. n1
auf Konto-Nr. n2
Betrag: b EUR
```

Diese kurze Nachricht sendet der Bankkunde an die Bank. Weitere Details einer realen Überweisung (Bankleitzahl, Inhaber des Zielkontos, Cents) spielen für unsere Betrachtungen keine Rolle bzw. können in eines der Felder einkodiert werden. Wir gehen davon aus, dass der Angreifer eines der Felder $n1$, $n2$ bzw. b manipulieren möchte (z. B. seine Konto-Nr. in $n2$ eintragen) und wollen dies verhindern. Nicht verhindern können wir, dass der Angreifer die Nachricht unterdrückt, indem er die Kommunikation an sich unterbindet. Sollte jedoch eine Überweisung bei der Bank ankommen, soll diese nur ausgeführt werden, wenn sie vom Bankkunden stammt; es reiche nicht, dass sie ohne sein Zutun vom PC abgesandt wurde.

3 Visuelle Kryptographie

3.1 Einführung

Visuelle Kryptographie wurde von Naor und Shamir [6] erstmalig beschrieben. Die Grundidee besteht darin, ein schwarz-weißes gepixeltes Bild so in zwei Teilbilder zu zerlegen, dass beide Teile für sich betrachtet ein zufälliges Muster aufweisen. Diese Teilbilder können auf transparente Folien gedruckt werden, die später übereinander gelegt werden, um die ursprüngliche Bildinformation zu erhalten. Es kann leicht gezeigt werden, dass diese Methode dieselben Sicherheitseigenschaften aufweist wie der *One-Time-Pad* (Vernam-Chiffre[2]), d. h. wir erhalten ein symmetrisches Verschlüsselungsverfahren mit informationstheoretischer Sicherheit (und akzeptieren Schlüssel, die Nachrichtenlänge aufweisen).

[2] Dieses Verfahren verschlüsselt jedes Zeichen (bzw. Bit) mit einem zufälligen Zeichen (Bit). Der Schlüssel wird nur einmal verwendet und ist genau so lang wie der Klartext. Das Verfahren ist dann nachweisbar nicht zu brechen, da im Chiffrat keine Information über den Klartext enthalten ist. Für viele

Dieses Sicherheitsniveau stellt das Maximum dar, denn selbst mit unbegrenzter Rechenzeit kann das Geheimnis nicht aus einem Teilbild gewonnen werden, weil zu nur einem gegeben Teilbild noch jede beliebige Nachricht, die mit derselben Anzahl Pixel dargestellt werden kann, *passen* würde.

Die geheime Nachricht wird (anschaulich formuliert) in zwei Folien bzw. eine Folie und ein Blatt Papier gleicher Größe zerlegt, die jeweils für sich betrachtet kein Bit Information über den Inhalt der Nachricht enthalten. Nur wer im Besitz beider Teile ist, kann die verschlüsselte Nachricht lesen.

Für unsere Anwendung interessant ist eine weitere Eigenschaft der visuellen Kryptographie: Das Entschlüsseln der Nachricht ist möglich, ohne die Hilfe eines Computers anwenden oder mathematische Operationen ausführen zu müssen. Der Vorgang des Übereinanderlegens der Folien ist rasch und ohne Expertenwissen ausführbar. Für die üblicherweise zur Absicherung von Online-Transaktionen verwendeten Kryptoverfahren gilt dies nicht, denn hier sind beim Entschlüsseln bzw. Verifizieren der Integrität einer Nachricht umfangreiche Berechnungen in Langzahlarithmetik auszuführen, die ein Mensch ohne technische Hilfe nicht leisten kann. Die Nutzung des PCs zur Ausführung der Operationen scheidet jedoch aus, wenn wir von der Existenz einer Malware ausgehen, denn der Angreifer ist in der Lage, kryptographische Operationen, die auf dem PC ausgeführt werden, so zu manipulieren, dass Verfälschungen einer Nachricht unbemerkt bleiben.

3.2 Anwendung visueller Kryptographie: VTANs

Wir wollen das Verfahren der visuellen Kryptographie nun nutzen, um Transaktionen abzusichern. Technisch werden wir das Verfahren so umsetzen, dass nur eine Folie eines Paares physikalisch erzeugt wird und dem Nutzer (Bankkunden) im Vorhinein als Einmal-Folie (visuelle TAN, kurz: VTAN) zur Verfügung gestellt wird. Die zweite Hälfte wird nichtphysikalisch an den Kunden in elektronischer Weise übertragen und lediglich am Monitor angezeigt. Erstmalig beschrieben wurde das hier vorgestellte Verfahren unabhängig von Borchert und Reinhard (nicht öffentlich dargestellt in [3]) sowie vom Autor dieses Beitrages [4].

Die VTANs sind vorbereitete, zufällige Pixelmuster, die auf ablösbare Folien gedruckt werden und ähnlich wie Transaktionsnummern dem Kunden auf Vorrat (unter Nutzung eines sicheren Kanals[3]) zur Verfügung gestellt werden. Die physikalische Größe der bedruckten Folie beträgt mehrere Quadratzentimeter, so dass auf einem Blatt mehrere VTANs mit laufender Nummerierung aufgebracht werden können. Soll im Verlauf einer Transaktionsübermittlung eine Nachricht von der Bank an den Kunden übertragen werden (nur diese Richtung ist vorgesehen), wird eine noch nicht benutzte VTAN bankseitig ausgewählt, das korrespondierende Pixelmuster berechnet und mit Angabe der VTAN-Nummer übertragen.

Anwendungen ist dieses Verfahren jedoch nicht praktikabel einsetzbar, da kein sicherer Kanal zur Übertragung der langen Schlüssel gegeben ist.

[3] Inwieweit einfache postalische Zustellung einen sicheren Kanal darstellt, ist diskussionswürdig. Bei Transaktionsnummern ist diese Zustellungsweise nicht ungewöhnlich, wobei meist zusätzlich weitere Mechanismen zur Aktivierung einer TAN-Liste hinzugezogen werden.

4 Problemlösung, VTANs

4.1 *Kreative Lösung*: Wir ignorieren das Problem

Die Kernidee zur Lösung des Problems, dass der Angreifer Herrschaft über den Rechner des Kunden besitzt, besteht darin, einen sicheren Kanal vom Rechner der Bank zum Auge (nicht PC) des Benutzers zu etablieren. Gelingt dies, ohne notwendige Annahmen zur Vertrauenswürdigkeit des PCs zu treffen, können wir die Malware ignorieren! Der PC wird dann zum Teil der Kommunikationsinfrastruktur, die ohnehin als unsicher vorausgesetzt wird (dies war die Motivation zur Einführung des SSL-TLS-Standards sowie von PINs und TANs beim Online-Banking).

Ein solcher Lösungsansatz ist durch Hinzunahme weiterer Geräte, die im Gegensatz zum PC als vertrauenswürdig angenommen werden, auf einfache Weise möglich. So kann die Visualisierung der Überweisungsdaten auf dem Display eines Kartenlesegerätes oder eines Mobiltelefons vorgenommen werden (solche Verfahren sind bereits im Einsatz). Diese Lösungen verschieben den Vertrauensanker weg vom PC auf eine andere Hardware, die nicht nur zusätzliche Kosten verursacht, sondern ihrerseits angreifbar sein könnte (Malware für Mobiltelefone ist bereits existent). Wir streben daher eine Lösung an, die ohne zusätzliche Hardware (abgesehen von bedrucktem Papier bzw. bedruckten Folien) realisierbar ist.

Kann der Bankkunde tatsächlich mit bloßem Auge die Integrität einer zu bestätigenden Transktion verifizieren, ohne auf die durch den PC bereitgestellten technischen Mechanismen vertrauen zu müssen, ist der Angreifer machtlos, denn die Malware auf dem Rechner kann nur diese Mechanismen beeinträchtigen. Es bleibt zu untersuchen, wie diese Transaktionssicherung vorgenommen wird und inwieweit der Nutzer zuverlässig eine Verifikation vornehmen kann.

4.2 Transaktionsprotokoll

Die Verschlüsselung und erfolgreiche Entschlüsselung einer Nachricht gibt keinen Hinweis darauf, dass diese Nachricht unverfälscht ist. Viele Kryptoverfahren erlauben die Manipulation einer verschlüsselten Nachricht ohne Kenntnis des geheimen Schlüssels. Bei visueller Kryptographie sind Manipulation besonders einfach, z. B. kann eine der Folien durch einen verfälschten Klartext ersetzt werden. Das Übereinanderlegen der beiden Folien wird dann diesen Klartext hervorbringen, da die zufälligen Pixel der zweiten Folie nur den Kontrast schmälern. Zwar könnte ein Mensch diesen simplen Angriff durch Betrachten der einzelnen Folien rasch bemerken, wir können dies aber nicht allgemein für alle Arten von Manipulationen voraussetzen. Die Verschlüsselung sorgt zuverlässig für die Vertraulichkeit von Nachrichten, Integritätssicherung ist die nächste Aufgabe.

Da die Vertraulichkeit übertragener Informationen keine Integrität bedingt, wird die Verwendung der VTAN nun in ein Protokoll eingebunden, dessen Ziel die Integritätssicherung von Transaktionen ist: Der Kunde initiiert den Vorgang, eine Transaktion (Überweisungsauftrag) zu übertragen[4]. Er trägt die Daten (die Felder $n1$, $n2$ bzw. b) in ein

[4]Dies kann wie üblich durch den Besuch der Webseite seiner Bank geschehen; alle weiteren Protokoll-

elektronisches Formular ein und übermittelt dieses an die Bank.

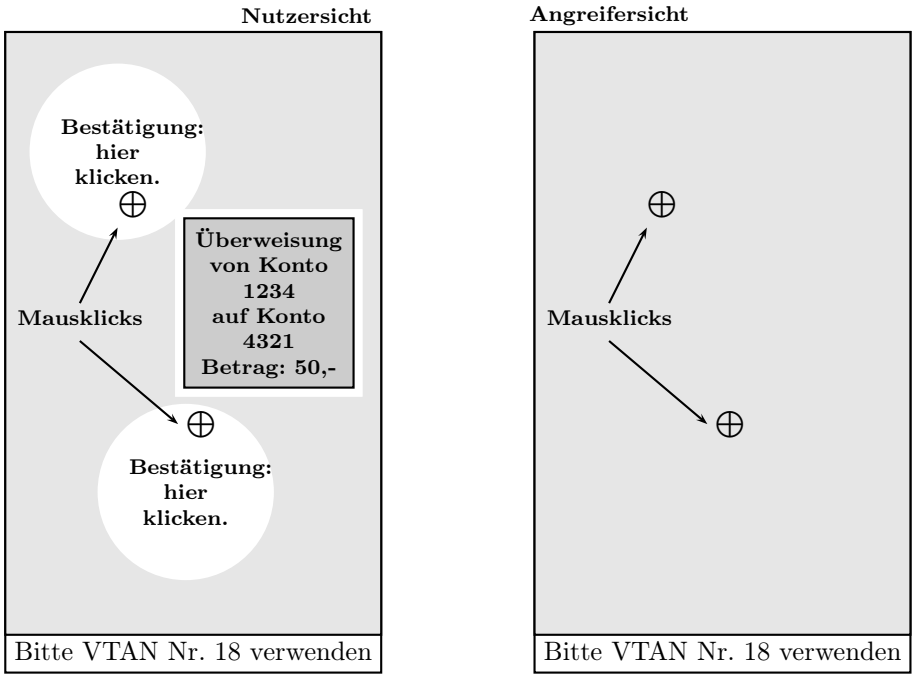

Abbildung 1: Transaktion mit VTANs

Die Bank wählt eine VTAN aus und antwortet mit dem durch visuelle Kryptographie berechneten Pixelmuster (siehe Abb. 1), das mittels dieser VTAN entschlüsselt werden kann (die Folie kann dazu vor den Monitor gehalten werden). In diesem Pixelmuster sind die beiden runden und das rechteckige Feld zufällig positioniert.

Der Kunde überprüft schließlich die Transaktionsdaten und bestätigt die Transaktion mit der Maus durch Anklicken der beiden runden Buttons. Die Bank überprüft, ob die Mausklicks innerhalb der Kreisflächen lokalisiert sind, und führt – falls die Überprüfung positiv verläuft – die Transaktion aus.

4.3 Sicherheitsbetrachtungen

Der Angreifer kann innerhalb oder zwischen den Protokollschritten eingreifen und Daten lesen, verändern bzw. unterdrücken. Zunächst stellen wir fest, dass er (bis zum Zeitpunkt der Mausklicks) keine Information über den Inhalt der Grafik hat, abgesehen von den darin einkodierten Transaktionsdaten, die er auf dem Kommunikationsweg (bzw. durch Malware auf dem PC) abgefangen hat bzw. aufgrund von ausgewerteten Transaktionen aus der Vergangenheit vermutet.

Um das Angriffsziel, die Übertragung und Bestätigung verfälschter Daten, zu erreichen, muss der Angreifer die falschen Daten zur Bank übertragen und anschließend die korrekt positionierten Mausklicks zur Bestätigung übermitteln.

schritte sind allein unter Nutzung von *HTTP* möglich.

Lässt der Angreifer die unverfälschten Transaktionsdaten an die Bank übermitteln, kann er sein Ziel nicht mehr erreichen, da im weiteren Protokolllauf nur noch diese Transaktion, aber keine andere bestätigt werden kann (ein Transaktionsabbruch würde nichts am *verbraucht*-Status der VTAN ändern).

Der Angreifer muss also bereits verfälschte Transaktionsdaten $(n1', n2', b')$ zur Bank übermitteln. Werden diese jedoch dem Kunden visualisiert, wird er keine bestätigenden Mausklicks tätigen, **sofern er in der Lage ist, die Veränderung zu erkennen**.

Der Angreifer muss daher entweder die Grafik so verfälschen, dass der Kunde erfolgreich getäuscht wird, oder die Mausklicks mithilfe von Malware selbst ausführen (durch Malware lassen sich die Mausklicks simulieren). Eine Verfälschung der Transaktionsdaten ist denkbar, da durch Ersetzen von Teilbereichen des Bildes durch zufällige Muster ein Löschen der Information (anschaulich: Überdecken mit grauer Fläche) möglich ist. Günstige Umstände (z. B. ähnliche Kontonummern, die der Angreifer aufgrund vermuteter Transaktionen vorbereitet haben kann) könnten diesen Angriff ermöglichen. Allerdings muss der Angreifer dazu die zufällige Position des rechteckigen Feldes erraten[5], was bei angenommener Gleichverteilung auf einer Menge von möglichen Positionen durch einen Sicherheitsparameter beschrieben werden kann. Hierbei kann man anstreben, dass der Parameter die Mächtigkeit der Menge, aus der eine herkömmliche TAN ausgewählt wird (z. B. 10^6), nicht unterschreitet, um an etablierte Sicherheitsniveaus anzuknüpfen.

Es bleibt die Betrachtung der Simulation der Mausklicks, wenn der Nutzer die Transaktion nicht bestätigt. Die Position der runden Felder kann in analoger Betrachtung zum rechteckigen Feld als gleichverteilt auf einer Menge möglicher Positionen angenommen werden. Die Ratewahrscheinlichkeit ist daher parametrisierbar und kann in den Rahmen bewährter Sicherheitsparameter aus dem Bereich Electronic Banking eingefügt werden.

Die erzielten Sicherheitseigenschaften stellen letztlich eine Verlängerung des normalerweise durch SSL-TLS abgesicherten Kanals zwischen PC und Bankrechner bis hin zum Auge des Benutzers selbst dar. Diese Kanalergänzung erlaubt es schließlich, den PC als Teil der Kommunikationsstrecke zwischen Kunde und Bank zu sehen, die durch Angriffe manipulierbar ist, aber durch kryptographische Mechanismen gesichert werden kann.

Der offensichtliche Schwachpunkt des vorgeschlagenen Verfahrens liegt in der prinzipiell begrenzten Fähigkeit des Nutzers, Manipulationen zu erkennen. Eine Überprüfung der Transaktionsdaten durch einen Menschen bietet breiten Raum für psychologisch motivierte Angriffsmechanismen. So können Unterschiede ähnlicher Ziffern bei künstlich verrauschten Grafiken kaum wahrgenommen werden; der Bankkunde wird jedoch nicht notwendigerweise misstrauisch, wenn die Darstellung durch den Angreifer gezielt gestört wird. Zudem sind sogenannte Zahlendreher oder verkürzte Zahlenfolgen (die durch Überdecken entstehen) für einen nicht immer voll konzentrierten Menschen nicht zuverlässig erkennbar, so dass dem Angreifer eine breite Angriffsfläche mithilfe von ähnlichen Kontonummern (oder Bankleitzahlen) geboten wird. Eine besondere Herausforderung läge darin, die Erfolgswahrscheinlichkeit solcher Angriffe zu quantifizieren, um einen Vergleich des Sicherheitsniveaus der VTANs mit anderen Mechanismen zu ermöglichen.

[5] Es wäre auch denkbar, dass der Angreifer viele kleine Veränderungen über die Grafik verteilt, ohne eine bestimmte Position des Rechtecks anzunehmen, was die Berechnung eines Parameters erschwert. Einem solchen Angriff kann man entgegenwirken, indem die ungenutzten Flächen der entschlüsselten Grafik ein optisches Muster aufweisen, das dann zerstört würde und die Verfälschung damit visualisiert.

4.4 Modifikationen und Erweiterungen

Das skizzierte VTAN-Verfahren kann für gegebene Sicherheitsparameter angepasst werden. So kann die Anzahl der inhaltlich zu verifizierenden, rechteckigen Felder erhöht werden, um die Trefferwahrscheinlichkeit beim Raten zu verringern; in gleicher Weise können auch andere Anzahlen der runden Bestätigungsfelder, die alle zur Bestätigung angeklickt werden müssen, vorgesehen werden.

Die VTANs selbst können ihre Information mehrfach übereinander gedruckt enthalten, um beispielsweise unterschiedliche Skalierungen (für 17"-, 19"-Monitore...) zu enthalten. Dies ist unbegrenzt möglich, führt aber bei jeder Zunahme einer weiteren Skalierung zu abnehmendem Kontrast der entschlüsselten Grafik.

Literatur

[1] A. Adelsbach, S. Gajek, and J. Schwenk. Visual Spoofing of SSL Protected Web Sites and Effective Countermeasures. In *Information Security Practice and Experience Conference*, volume 3439 of *Lecture Notes in Computer Science*, pages 204–216. Springer, 2005.

[2] BdB. Bundesverband deutscher Banken (Hrsg.): Online-Banking-Sicherheit: Informationen für Nutzer, Sep 2006. online: `www.bdb.de/pic/artikelpic/092006/06_09_OnlineBankingSicherheit.pdf`.

[3] Bernd Borchert and Klaus Reinhardt. Deutsches Patent- und Markenamt: Abhör- und manipulationssichere Verschlüsselung für Online Accounts mittels Visueller Krytographie an der Bildschirmoberfläche (Patenteinreichung DE-10-2007-018802.3), 2007.

[4] Ulrich Greveler. VTANs – eine Anwendung visueller Kryptographie in der Online-Sicherheit. In *Workshop Angewandte Kryptographie, Informatik 2007*, volume 110 of *Lecture Notes in Informatics*. Köllen, 2007.

[5] Avivah Litan. Increased Phishing and Online Attacks Cause Dip in Consumer Confidence, June 2005. Gartner Report, Number: G00129146.

[6] M. Naor and A. Shamir. Visual Cryptography. In Alfredo De Santis, editor, *Advances in Cryptology – EUROCRYPT '94*, volume 950 of *Lecture Notes in Computer Science*, pages 1–12. Springer.

[7] Alan D. Smith. Exploring security and comfort issues associated with online banking. *International Journal of Electronic Finance.*, (1):18–48, 2006.