VTANs – Eine Anwendung visueller Kryptographie in der Online-Sicherheit

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

Abstract: Wir beschreiben ein Verfahren, das die authentische Online-Übertragung von Transaktionen ermöglicht, ohne dass ein vertrauenswürdiger Zustand des Endgeräts (PC) vorausgesetzt wird. Das Verfahren 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 (Authentisierung, Verschlüsselung) entgegengewirkt wird.

In den letzen Jahren wurde vermehrt über Angriffe berichtet [Lit05], die den Bankkunden im Visier haben und ihn dazu bringen sollen, geheime Autorisierungsdaten an die Angreifer herauszugeben (z. B. Phishing). Durch gezielte Täuschung mit technischen Mitteln wie z. B. *Visual Spoofing* [AGS05] oder auch durch trickreich formulierte 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 [BdB06].

2 Angreifermodell und zu schützende Transaktion

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 unbeschränkte Herrschaft über den PC des Kunden (über Malware).

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 von seinem PC abgesandt wurde.

3 Visuelle Kryptographie

3.1 Einführung

Visuelle Kryptographie wurde von Naor und Shamir [NS94] 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), d. h. wir erhalten ein symmetrisches Verschlüsselungsverfahren mit informationstheoretischer Sicherheit (und akzeptieren Schlüssel, die Nachrichtenlänge aufweisen).

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.

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.

Die VTANs sind daher vorbereitete, zufällige Pixelmuster, die auf ablösbare Folien gedruckt werden und ähnlich wie Transaktionsnummern dem Kunden auf Vorrat (unter Nutzung eines sicheren Kanals[1]) 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-Nr. übertragen.

4 Protokollablauf und Sicherheitsbetrachtung

4.1 Transaktionsprotokoll

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[2]. Er trägt die Daten (die Felder $n1$, $n2$ bzw. b) in ein elektronisches Formular ein und übermittelt dieses an die Bank.

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.

[1] 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.

[2] Dies kann wie üblich durch den Besuch der Webseite seiner Bank geschehen; alle weiteren Protokollschritte sind allein unter Nutzung von *HTTP* möglich.

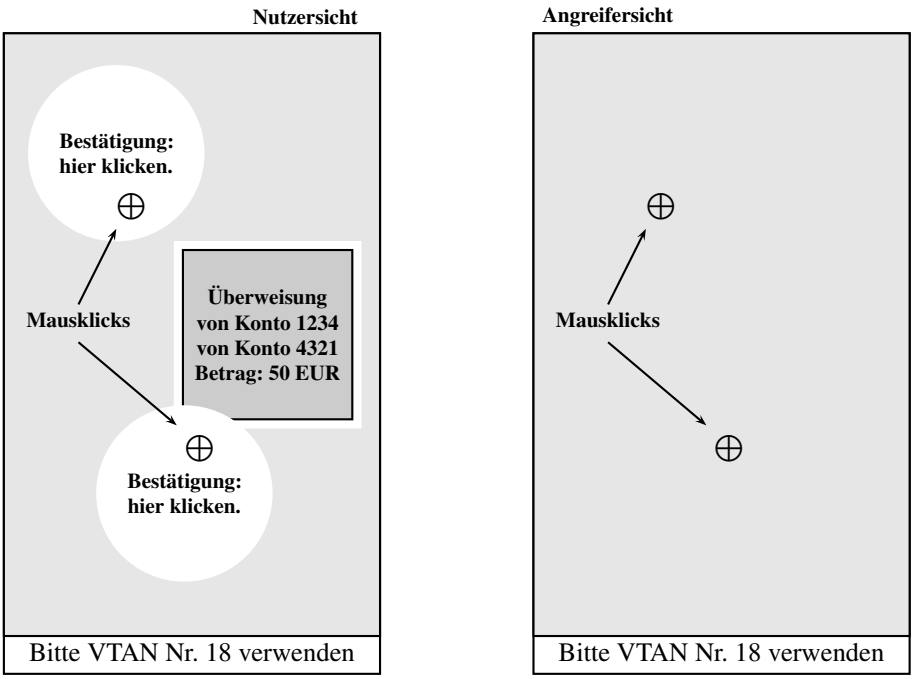

Abbildung 1: Transaktion mit VTANs

4.2 Sicherheitsanalyse

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 haben kann.

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.

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. 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 simulieren). Eine Verfälschung der Transaktionsdaten ist denk-

bar, da durch Ersetzen von Teilbereichen des Bildes durch zufällige Muster ein Löschen der Information (überdecken mit grauer Fläche) möglich ist. Günstige Umstände (z. B. ähnliche Kontonummern) könnten diesen Angriff ermöglichen. Allerdings muss der Angreifer dazu die zufällige Position des rechteckigen Feldes erraten[3], 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 Position 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 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 mit kryptographische Mechanismen gesichert werden kann.

4.3 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

[AGS05] A. Adelsbach, S. Gajek und J. Schwenk. Visual Spoofing of SSL Protected Web Sites and Effective Countermeasures. In *Information Security Practice and Experience Conference*, 2005.

[BdB06] BdB. Bundesverband deutscher Banken (Hrsg.): Online-Banking-Sicherheit: Informationen für Nutzer, Sep 2006.

[Lit05] Avivah Litan. Increased Phishing and Online Attacks Cause Dip in Consumer Confidence, June 2005.

[NS94] M. Naor und A. Shamir. Visual cryptography. In *Advances in Cryptology – EUROCRYPT ’94, LNCS 950*. Springer, 1994.

[3] 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 jedoch entgegenwirken, indem die ungenutzten Flächen der entschlüsselten Grafik ein optisches Muster aufweisen, das dann zerstört würde und die Verfälschung damit visualisiert.