Investigation on Security Aspects in Online Payment Systems

Gregor Pumberger, Michal Wasilewski

{G.Pumberger, Michal.Wasilewski}@Gmx.at

Abstract. In Zeiten wo der Internethandel immer populärer wird, nimmt auch die Anzahl der Zahlungsmöglichkeiten im WWW zu, welche klassische Zahlungsformen (Erlagschein etc.) immer mehr ersetzen[3]. Da die Anzahl von Malware und Angriffen auf fremde Rechner ebenso rapide steigt, ist es gerade bei online Zahlungen wichtig, dass diese sicher durchgeführt werden können. In diesem Paper werden benötigte Sicherheitsvorkehrungen besprochen und eine Auswahl von verschiedenen populären online Zahlungsanbietern vorgestellt und miteinander verglichen.

Keywords: Online Payment Sicherheit, Sicherheitskriterien, Überweisung, eWallet, mobile Payment, Prepaid, Kredit-/Bankomatkarten Transaktionen

1 Einleitung

Das Ziel der Evaluierung von Online Payment Systemen ist, sowohl die Stärken als auch die Schwächen der zum Einsatz kommenden Sicherheitsvorkehrungen anzuzeigen. Eine derartige Betrachtung nimmt gerade in unseren Zeiten an Bedeutung zu, da es für immer mehr Unternehmen nahezu existenzwichtig ist, derartige Systeme "sicher" einsetzen zu können[4]. Jedoch müssen Unternehmen, die Dienstleistungen und Güter über das Internet vertreiben oftmals den Mittelweg zwischen Sicherheit, Ausmaß der Zahlungen und Benutzerfreundlichkeit gehen[1].

In Kapitel 2 werden Kriterien betrachtet die ein Online Payment System zu erfüllen hat, um als solches Anerkennung finden zu können. Oftmals sind dabei auch länderspezifische Aspekte, wie zum Beispiel Unterschiede der Rechtssysteme zu beachten.[6] Die Aspekte dieses Kriterienkatalogs wurde von den Autoren ausgewählt und stellt deshalb keinen Anspruch auf Vollständigkeit aller wichtigen Kriterien.

In Kapitel 3, "Anbieter Übersicht" wird auf die unterschiedlichen Anbieter von Online Payment Systemen eingegangen und diese näher betrachtet.

Diese Evaluierungsmaßnahme wird anschließend mit der Theorie in Zusammenhang gebracht und diskutiert.

2 Kriterien

Das wichtigste Kriterium, welches ein Online Payment System zu erfüllen hat, ist eine sichere Datenübertragung von den Kundendaten zum Server des Anbieters, da das

beste Sicherheitssystem sinnlos ist, wenn die Daten einfach abgefangen werden können. Für eine sichere Client-Server Kommunikation bietet sich das wohl bekannteste Verfahren für Kommunikations-Protokolle, HTTPS/SSLv3 128/256-Bit Verschlüsselung mit einem SSL-Zertifikat einer namhaften Firma wie z.B: VeriSign an[8].

Die Kunden Authentifizierung sollte nicht nur durch ein statisches Passwort, welches durch Malware(Keylogger) mitprotokolliert werden kann, abgesichert sein. Es sollte auch noch ein dynamischer Code Verwendung finden, welcher am besten durch ein externes Gerät generiert wird. Dieser kann mittels eines Security-Token oder auch über SMS (mobileTAN) erfolgen.

Des Weiteren sind Konsistenz der Informationen (hinsichtlich Höhe, Ausführungszeitpunkt und Zweck der Transaktion), Totalität (im Falle unbeabsichtigter Datenkorruption darf keine Zahlung erfolgen) und Nichtbestreitbarkeit zu gewährleisten. [9]

3 Anbieter Übersicht

3.1 Überweisungen

3.1.1 EPS

Der Electronic Payment Standard ist die Schnittstelle in die Online-Zahlungssysteme der österreichischen Banken und ermöglicht das schnelle und sichere Online Bezahlen im Internet mittels vertrauter Online-Banking-Systeme und ist mit keinen zusätzlichen Kosten verbunden. Somit ist keine zusätzliche Registrierung oder Zugangs-Code erforderlich. Der Kunde wählt als Zahlungsmethode „eps“ und die kontoführende Bank aus. Nun wird eine Verbindung zum Internet-Banking Portal hergestellt. Hier meldet sich der Benutzer mittels gewohnter Benutzerkennung und PIN oder Digitaler Unterschrift an. Rechnungsdaten werden automatisch an das Internet-Banking System übermittelt - manuelle Eingaben sind nicht erforderlich! Der Auftrag wird mittels TAN oder Digitaler Unterschrift bestätigt. Die Bank leitet die Zahlung an den Händler weiter. Damit ist die Bezahlung abgeschlossen.

Die Spezifikation der Schnittstelle legt die technischen Anforderungen für den Datenaustausch fest:

Der Basis-Datencontainer zur Abwicklung der Online Zahlung wird durch ein XML-Schema, das auf den W3C Standard aufbaut, definiert.

Der Nachrichtenaustausch basiert auf HTTP- und HTTPS-Protokollen (SSL/TLS).

Alle URL-Angaben, die für die Abwicklung des EPS-Ablaufs notwendig sind, werden an die Bank übermittelt. Die URLs müssen von der Behörde (Händler) UTF-8 kodiert werden. Die Kommunikation ist mit einem Session Time Out abgesichert.

Der Datencontainer der elektronischen Zahlungsbestätigung der Bank ist durch bestimmte Datenelemente definiert (Inhalt, Banksignatur mit X.509v3 Zertifikat).

3.1.2 Sofortüberweisung

Auch bei diesem System verwendet der Benutzer seine Online-Banking-Zugangsdaten (Benutzername, Zugangskennwort, TAN) jedoch gibt er diese nicht über das eigene Bankenportal ein, sondern über eine Zwischenstelle wie zum Beispiel www.payment-network.com

Der überwiesene Betrag wird beim Geschäftspartner zeitgleich zugebucht.

3.2 Mobile Payment

3.2.1 paybox

Paybox wurde für das bezahlen kleiner Beträge im Alltag eingeführt und ist somit keine klassische online Zahlungsmethode, jedoch nimmt die Akzeptanz von paybox in online Shops immer mehr zu.

Bei der Bezahlung mit paybox, erhält man einen automatischen Anruf oder eine SMS von paybox mit dem Betrag und Zahlungsempfänger. Bei einem Anruf wird die Zahlung durch die Eingabe eines paybox PINs freigegeben und bei einer SMS mittels einer Antwort SMS mit dem Text „JA“. Daraufhin wird die Zahlung sofort freigegeben und die Abrechnung erfolgt über die Handyrechnung oder über das Bankkonto.

Für die Nutzung des Service ist eine Registrierung nötig, wobei eine jährliche Gebühr zu bezahlen ist.

3.3 eWallets

Wie der Name eWallet schon vermuten lässt, handelt es sich hierbei um eine Art elektronische Geldbörse, welche durch verschiedene Einzahlungsmöglichkeiten aufgeladen werden kann. Alle hier aufgeführten Anbieter verwenden zum Login zumindest eine Authentifizierung mittels Benutzername und Passwort, welches über eine 128-Bit SSL Verbindung übertragen wird. Die Zahlungen sind in der Regel für den Kunden kostenlos.

3.3.1 PayPal

Paypal ist das wohl größte und bekannteste online Wallet. Bei einer Bezahlung mittels PayPal wird man zur PayPal Seite weitergeleitet, wo man sich mit seiner E-mail Adresse und Passwort einloggen muss, um daraufhin die Bezahlung (Betrag + Empfänger) zu bestätigen und eine Zahlungsmethode auszuwählen.

Der Betrag kann mittels Guthaben, registriertem Bankkontoeinzug oder registrierter Kreditkarte ohne weitere Eingabe von CVS Code oder PINs etc. bezahlt werden.

Als weiteres Sicherheitsfeature bietet PayPal seit kurzem zusätzlich zur Authentifizierung mittels Benutzername und Passwort die Eingabe eines Sicherheitsschlüssels ein. Der Sicherheitsschlüssel wird mittels eines OTP(=One Time

Password)-Sicherheitstoken[1] generiert oder auf das zuvor registrierte Mobiltelefon per SMS gesendet.

Jeder Code ist einmalig und nach der Generierung nur 1 Minute lang gültig. Leider erlaubt es PayPal sich trotz aktiviertem Login mit Sicherheitsschlüssel, sich ohne diesen einzuloggen, indem man seine Sicherheitsfrage beantwortet oder die komplette Kreditkartennummer eingibt.

3.3.2 Moneybookers

Die Bezahlung mittels Moneybookers, funktioniert analog zu der Bezahlung mit PayPal (Weiterleitung zur Moneybookers Seite → Bezahlung). Es ist auch eine direkt Zahlung mittels verifizierter Kreditkarte oder mittels zuvor aufgeladenen Guthaben möglich. Zusätzlich zum Login mittels Benutzernamen und Passwort ist die Eingabe eines Turing Code Captchas nötig.

3.3.3 Neteller

Bei einer Bezahlung mittels Neteller, ist die Eingabe der Konto-ID und einer sicheren ID(eine Art zweites Passwort) notwendig. Es erfolgt keine Weiterleitung zur Neteller Seite.

Die Bezahlung ist nur möglich, wenn sich im Neteller Account genügend Guthaben befindet. Um sein Neteller Guthaben aufzufüllen, muss man sich auf der Neteller Seite mittels Konto-ID, Sicherer-ID und Passwort einloggen. Ein weiteres Sicherheitsfeature von Neteller ist, falls von einer IP-Adresse welche nicht vom registrierten Land des Kunden stammt ein Zugriffsversuch erfolgt, wird der Account eingefroren und kann nur durch eine Verifizierung durch den Support wieder geöffnet werden.

3.3.4 ClickandBuy

ClickandBuy bietet länderspezifische Abwicklungsoptionen. Der Nutzer kann zum Beispiel in Österreich die Abrechnung mittels monatlicher Zahlung per Lastschrift, Kredit-/Debitkarte, online Banküberweisung/EPS, lokale Banküberweisung oder Rechnung begleichen.

Um eine Zahlung vornehmen zu können muss sich der Benutzer bei ClickandBuy registrieren und Abrechnungsoptionen definieren. Nun kann der Benutzer kostenpflichtige Dienste im Internet konsumieren, wobei der Zahlvorgang durch eine Zwischenseite von ClickandBuy, welche Anbieter, Preis und Datum dokumentiert, abgewickelt wird.

Bereits während des Registrierungsprozesses werden Prüfungen für folgende Eingaben durchgeführt:

e-Mail Adresse, Adresse (weltweit), Dublettenprüfung, Real Time Online Prüfung von Kreditkartendaten (CVV/AVS Checks bei Kreditkartenregistrierungen), Prüfung von Bankdaten durch das PIN-Code Verfahren, Bonitätsprüfung, IP-Adressen Prüfung.

Zusätzliche erfolgen Prüfungen von Restriktionen, die individuell durch den Fraud Server festgelegt werden können: Länderrestriktionen, Branchenrestriktionen.

---

1 Folgendes Modell kommt derzeit (01/2009) bei PayPal zum Einsatz http://www.aladdin.com/etoken/devices/pass.aspx

Interne Prüfungsregeln kommen zum Einsatz, die durch das Fraud Team aufgrund von Erfahrungswerten und arithmetischen Logiken festgelegt werden

Daraus ergeben sich variable Anpassungen der White und Black List

3.4 Prepaid

3.4.1 paysafecard

Bei der Paysafecard handelt es sich um eine Prepaid-Karte (Rubbelkarte), der ein bestimmtes Guthaben zugeordnet ist. Analog zu Mobilfunkkarten sind beim Einsatz der Paysafecard keine Angaben von Benutzerinformationen erforderlich, es ist lediglich der 16-stellige Rubbelcode, der sich auf der Rückseite der Karte befindet für den Bezahlvorgang von Bedeutung. Bei Zahlung mittels Paysafecard wird über den Paysafecard-Server das Kartenguthaben überprüft. Falls der Rechnungsbetrag das Guthaben übersteigt wir der Benutzer aufgefordert eine weitere Karte zu verwenden (max. 10Karten pro Zahlung möglich). Erst wenn der Händler die Auslieferung dieses Produkts bestätigt hat, wird das "reservierte Guthaben" endgültig von der Karte des Kunden abgezogen.

Falls ein Händler die bestellte und bezahlte Ware innerhalb einer gewissen Frist nicht liefern sollte, wird das für diese Ware "reservierte Guthaben" auf der Karte dem Kunden wieder freigegeben.

Um das Guthaben der Karte besser absichern zu können, kann zusätzlich ein Passwort vergeben werden. Es ist auch möglich eine Geheimfrage zu definieren, um bei vergessenem Passwort auf das Guthaben zugreifen zu können.

Da der Kunde zur eigentlichen Zahlungsabwicklung immer auf den Paysafecard-Server geleitet wird, gibt er erst dort seinen PIN-Code und sein Passwort ein. Da bereits bei Kauf die Ware bezahlt wird entfällt für den Händler das Risiko dass der Kunde nach Erhalt der Waren diese nicht bezahlt. Diese Bezahlmethode ist vor allem für Jugendliche und Benutzer ohne Kreditkarte interessant.

Alle Datenübertragungen - sowohl zwischen Kunde und Paysafecard als auch Paysafecard und Händler - finden verschlüsselt statt, Kodierungssystem ist dabei der SSLv3 Standard.

3.4.2 @Quick

Um @Quick, welches von PayLife angeboten wird, nützen zu können, muss die Quickkarte aufgeladen und ein Kartenlesegerät vorhanden sein. Nach der Weiterleitung zur Anbieterseite braucht man nur noch auf “Bezahlen” gehen und der Betrag wird vom Quickguthaben abgebucht.

3.5 Kredit- & Bankomatkarten Services(von PayLife & CardComplete)

3.5.1 Verified by Visa/MasterCard SecureCode

PayLife & CardComplete bieten beide die Zahlungsmöglichkeiten MasterCard SecureCode und Verified by VISA an, welches einen zusätzlichen Passwortschutz zur herkömmlichen Kreditkartenzahlung hinzufügt [2].

Hierbei muss die Kreditkarte für SecureCode bzw. Verified by VISA freigeschalten und ein Passwort gewählt werden.

Bei einer Bezahlung wird der Kunde auf eine Seite des Anbieters (PayLife oder CardComplete) weitergeleitet. Der Kunde muss zusätzlich zu seinen Kreditkarten Informationen wie Nummer, Ablaufdatum und CVS Code zusätzlich ein Passwort eingeben. Verkäufer sowie Kunde werden durch 3-D Secure-Technologie[2] eindeutig authentifiziert und die Daten werden über eine sichere SSL/TLS Verbindung übertragen[5].

3.5.2 Maestro SecureCode

Von PayLife werden zusätzlich noch Maestro SecureCode und @Quick[3] angeboten.

Bei Maestro SecureCode, muss man zuerst die Bankomat Karte für dieses Service freischalten lassen und ein Passwort(Secure Code) wählen. Die Bezahlung funktioniert dann wie bei MasterCard SecureCode, nur dass anstatt den Kreditkarteninformationen die Bankomartkartennummer, Ablaufdatum und das Passwort eingegeben werden müssen.

4 Evaluierung

Table 1. Vergleich der Anbieter

	Daten-übetragung	**Authentifi-zierung**	**offline Komponente**	**dynamische Komp.**	**Registrier-ung**
EPS/ Sofortüw.	SSL/TLS	Benutzer Nr., PW/digitale Unterschrift, TAN	TAN, digit. Unterschrift	TAN	Nein
Paybox	SSL/GSM	SMS/ Anruf(PIN)	SMS/Anruf	SMS/Anruf	Ja
PayPal	SSL	e-Mail,PW, Security Token[4]	Security Token	Security Token	Ja
Money-bookers	SSL	e-Mail,PW, CAPTCHA	-	-	Ja
Neteller	SSL	Benutzer-ID, Sichere ID	-	-	Ja
ClickandBuy	SSL	e-Mail, PW,	-	-	Ja

2 grafische Darstellung siehe [5] Figure 2 & 3

3 siehe 3.4.2

4 Optional Verfügbar

		CAPTCHA			
paysafecard	SSL	Code, PIN	Karte(Code)	-	Nein
@Quick	SSL/TLS	Karte	Karte	-	Nein
Verified by Visa/ MasterCard SecureCode	SSL/TLS	3D-Secure Tech.,KK-Nr, CVS, Ablaufdat., Code	-	-	Ja
Maestro Secure Code	SSL/ TLS	Kartennr, Ablaufdatum, Code	-	-	Ja

Wie aus Tabelle 1 hervorgeht, erfüllen zurzeit nur die Überweisungsdienste EPS /Sofortüberweisung sowie paybox alle Punkte des zuvor aufgestellten Kriterienkatalogs. Wobei paybox die Nachteile einer Registrierung sowie zusätzlichen Kosten gegenüber den Überweisungs-Varianten mit sich bringt.

Von den anderen Diensten kommt PayPal mit der Einführung eines Sicherheitsschlüssels als einziger Anbieter nahe an die geforderten Kriterien heran. Dieses von PayPal angebotene Zusatzfeature ist jedoch nur optional und lässt sich wie zuvor beschrieben, relativ leicht umgehen.

5 Schlussfolgerung

Da sich bei online Zahlungen nicht nur ein Standard durchgesetzt hat, sondern von vielen Benutzern für verschiedene Transaktionen, verschiedene Zahlungsdienste in Anspruch genommen werden, sollten alle Dienste so sicher wie möglich gehalten werden[7]. Es wäre durchaus wünschenswert, dass gerade E-Payment-Systeme wie Kreditkartenzahlungen zusätzlich durch dynamische Komponenten abgesichert wären, da diese Zahlungsarten der enormen Gefahr von Missbrauch, wie Abfangen von Kundendaten, durch Phishing-Seiten und Keyloggern, ausgesetzt sind.

Weiters sollte auch nicht außer Acht gelassen werden, dass immer auch ein hohes Sicherheitsrisiko auf der Benutzerseite besteht. Deshalb sollte auf der Client Seite beachtet werden, dass der Rechner frei von Malware bleibt und immer sichere Passwörter zu wählen sind. Jeder Anbieter eines E-Payment-Systems muss die Balance zwischen technisch möglicher Absicherung der Transaktionen und Aufwand den der Benutzer bei einer Zahlung auf sich nehmen muss aufwiegen. Offenbar ist für den Großteil der Benutzer, jener Systeme, alleinig die „gefühlte“ Sicherheit für die Wahl der Variante ausschlaggebend.

References

1. Jones, S., Wilikens, M., Morris, P., Masera, M.: Trust requirements in e-business. Communications of the ACM, vol. 43, Issue 12, pp. 81-97. ACM (2000)

2. Banerjee, S., Karforma, S.: A prototype design for DRM based credit card transaction in E-commerce. Ubiquity, vol. 9, Issue 18, Article No. 2, ACM (2008)
3. Mann, R.J.: Regulating Internet payment intermediaries, ACM International Conference Proceeding Series; Vol. 50, Proceedings of the 5th international conference on Electronic commerce, pp. 376-386, Pittsburgh, Pennsylvania (2003)
4. Chau, P.Y.K., Poon, S.: Octopus: an e-cash payment system success story, Communications of the ACM, vol. 46, Issue 9, pp. 129-133. ACM (2003)
5. Pasupathinathan, V., Pieprzyk, J., Wang, H., Cho, J.Y.:
Formal analysis of card-based payment systems in mobile devices, ACM International Conference Proceeding Series; Vol. 167, Proceedings of the 2006 Australasian workshops on Grid computing and e-research – Vol. 54, pp. 213 – 220, Hobart, Tasmania, Australia (2006)
6. Peha, J.M., Khamitov, I.M.: PayCash: a secure efficient Internet payment system, ACM International Conference Proceeding Series; Vol. 50, Proceedings of the 5th international conference on Electronic commerce, pp. 125-130, Pittsburgh, Pennsylvania(2003)
7. MacKie-Mason, J.K., White, K.: Evaluating and Selecting Digital Payment Mechanisms, University of Michigan (1996)
8. Ureche, O.: Digital payment systems for Internet commerce: The state of the art , World Wide Web, vol. 3, Number 1, Springer Netherlands (2006)
9. Heng, S.: E-Payment-Systeme: Treiber einer notwendigen Evolution der Zahlungssysteme, Handbuch E-Money, E-Payment & M-Payment, Part 4, Physica-Verlag HD (2006)