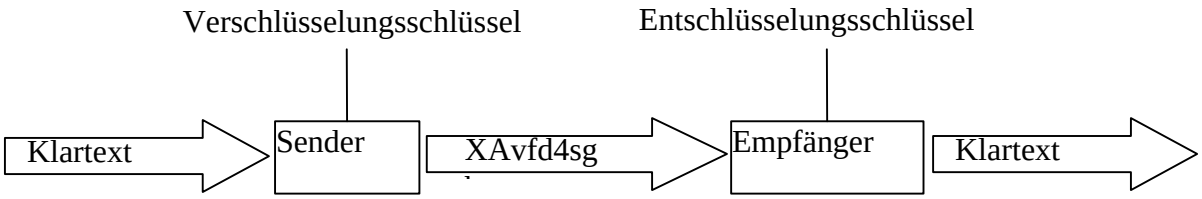
Inhalt:

Einleitung:

Im Moment kann man überall ein das Schlagwort E-Commerce hören. Die Unternehmer versuchen schon jetzt sich ihre feste Position auf dem digitalen Marktplatz zu sichern. E-Commerce Unternehmen sprießen aus dem Boden und bekommt so manche Vision zu hören, das E-Commerce den normalen Handel in Zukunft komplett ersetzten wird.
Doch wie steht es mit der Datensicherheit in diesem Sektor. Immer häufiger werden immer größere Summen auf elektronischem Wege verschoben. Dies setzt ein sichere Infrastruktur voraus. Häufig ist es auch so, dass Sicherheitssysteme sehr kostspielig sind und deshalb wird gerade in diesem Bereich häufig auf kostengünstigere „unsichere" Systeme zurückgegriffen. Hier soll nun versucht werden sicherheitsrelevante Probleme aufzuzeigen, und kurz auf verwendete Techniken zum Schutz der Daten einzugehen. Besonderes Augenmerk soll dabei auf den elektronischen Zahlungssystemen liegen, da gerade bei diese Systeme Sicherheitsprobleme fatale Folgen haben können, für den Kunden wie auch für den Händler. Da diese Materie sehr weitreichend ist, sollte dies nur als ein gröber Überblick angesehen werden und dem Interessierten als Startpunkt dienen. Auf weiterführenden Themen wird aber im allgemeinen mit Schlagwörtern verwiesen.

1. Einführung in die Kryptographie:

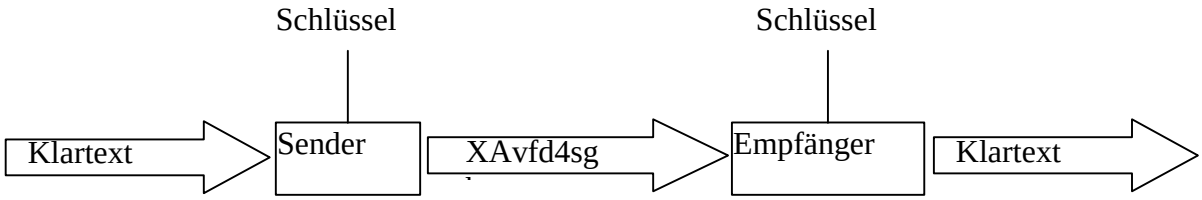
Unter Verschlüsselung versteht man ein Verfahren zur sicheren Übertragung von sensiblen Informationen über im allgemeinen unsichere Medien. Dabei wird unter Verwendung eines Verschlüsselungsschlüssels der Klartext in einen Geheimtext umgewandelt. Nun kann er sorglos über das unsichere Medium transportiert werden, ohne dass ein Unbefugter den Text entziffern kann. Ist der Geheimtext unversehrt beim Empfänger angekommen, kann dieser den Geheimtext mit Hilfe eines Entschlüsselungsschlüssels wieder in den ursprünglichen Klartext umwandeln.



In der Kryptographie unterscheidet man im allgemeinen zwischen zwei verschiedenen Verfahren, den Symmetrischen Verschlüsselungsverfahren und den Asymmetrischen Verfahren.

1.1 Symmetrische Verschlüsselungsverfahren:

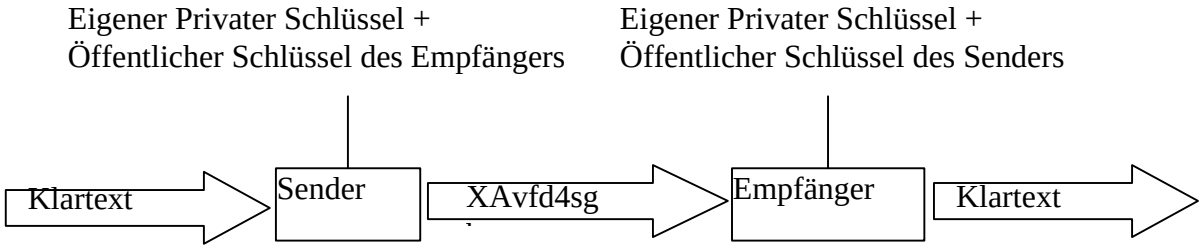
Wird zur Verschlüsselung sowie zur Entschlüsselung der gleiche Schlüssel verwendet, so nennt man dies ein symmetrisches Verfahren.



Die wichtigsten Vertreter dieser Gattung sind DES (Data Encryption Standard) entwickelt 1977 in den USA, IDEA (International Data Encrytion Algorithm) sowie der RC5 Algorithmus (1994 von Ron Rivest vorgestellt).
Von den oben genannten Verfahren ist wohl DES das mit Abstand am weitesten verbreitete Verfahren und gilt bis heute als sehr sicher. Das Problem von DES liegt darin, das bei der Entwicklung von DES eine feste Schlüssellänge von nur 56 Bit festgelegt wurde. Diese Einschränkung ermöglicht es, das mit heutigen Hochleistungsrechnern in kurzer Zeit einfach alle Schlüssel durchprobiert werden können, einen sogenannten Brute Force Angriff.
Allgemein ergibt sich bei den symmetrischen Verfahren folgendes Problem. Sender und Empfänger müssen über den gleichen Schlüssel verfügen, d.h. der Schlüssel muss entweder vorher abgesprochen sein oder über eine sichere Leitung übertragen werden., über die man dann ja auch gleich die Nachricht übermitteln könnte. Diese sichere Leitung ist meistens nicht gegeben.

1.2 Asymmetrische Verschlüsselungsverfahren:

Bei den asymmetrischen Verschlüsselungsverfahren werden zur Ver- und Entschlüsselung zwei verschiedene Schlüssel benötigt. Der Sender kann die Nachricht mit einem sogenannten öffentlichen Schlüssel des Empfängers verschlüsseln. Eine so verschlüsselte Nachricht kann nur der Besitzer des passenden privaten Schlüssels entschlüsseln, also der Empfänger.
Diese Verfahren wird deswegen häufig auch Public Key Verfahren genannt.



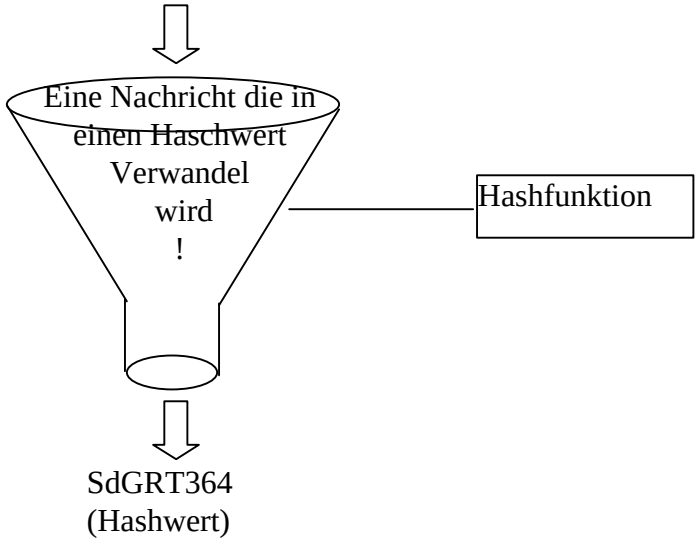
Die bekanntesten Verfahren sind hier RSA benannt nach ihren Entdeckern Ron Rivest, Adi Shamir und Leonard Adleman. Ein weiteres Verfahren, welches auch bei der E-Mail Verschlüsselungssoftware PGP zum Einsatz kommt ist das Diffie Hellman Verfahren.
Der Vorteil dieser Verfahren ist, das man keine Schlüssel untereinander austauschen muß, ja sogar seinen öffentlichen Schlüssel jedem preisgeben kann. Ein weiterer großer Vorteil ist, das man weiß von wem die Nachricht verschlüsselt wurde und somit ein Schutz vor gefälschten Nachrichten gewährleistet werden kann.
Ein Nachteil dieser Verfahren ist, dass sie sehr langsam in ihrer Durchführung sind und deshalb nur für kurze Nachrichten verwandet werden können.

1.3 Hybridverfahren:

Aus oben genannten Problemen der verschiedenen Verfahren wird häufig ein Hybridsystem eingesetzt. Dabei wird mit dem asymmetrischen Verfahren ein geheimer Schlüssel verschlüsselt und an den Empfänger übermittelt. Dieser Schlüssel kann nun benutzt werden, um große Datenmengen mit einem schnellem symmetrischen Verfahren zu verschlüsseln und zu übermitteln.

1.4 Hashing:

Um die Unveränderbarkeit von Daten zu gewährleisten gibt es leider keine Möglichkeit, die es zulassen würde, die Daten über Netze oder andere digitale Medien zu übermitteln. Dies liegt in der Beschaffenheit und der Funktionsweise der Netze. Daten müssen in Pakete unterteilt werden usw. Daten können also nicht absolut gegen Veränderungen geschützt werden. Man versucht hier nun einen anderen Lösungsansatz, die Erkennung von Veränderungen. Kann man wenigstens erkennen, dass Daten verändert wurden, so kann man diese verwerfen und neu anfordern. Hier kommen nun die Hashingverfahren zum Einsatz.
Ein Hashingverfahren nimmt eine Nachricht und berechnet über eine bestimmte Hashingfunktion einen zugehörigen Hashwert. Dieser Hashwert muss nun folgende Kriterien erfüllen. Es muss unmöglich sein zwei unterschiedliche Nachrichten mit dem selben Hashwert zu finden und aus dem Wert dürfen keine Rückschlüsse auf den Text zu ziehen sein. Häufig verwendet wird hier z.B. das SH1 Verfahren.



2. Allgemeine Probleme der Datensicherheit:

Beim E-Commerce ergeben sich ganz neue Problem, die im normalen Handel so nicht auftreten oder aber auf einfache Weise zu lösen sind. Im folgenden Abschnitt soll auf diese Probleme eingegangen werden.

2.1 Sichere Kommunikation:

Das Internet bieten von Haus aus keine Möglichkeiten zur sicheren Datenübertragung. Die Daten müssen viele verschiedene und zum Teil unbekannte Stationen passieren bevor sie ihren Zielort erreichen, um so wichtiger ist es für die Übertragung der Daten einen sicheren Übertragungskanal zu schaffen, gerade für den elektronischen Handel ist dies von größter Wichtigkeit, weil es hier um Geld geht und einem Betrug möglichst vorgebeugt werden muss. Um diesem Problem zu begegnen werden hauptsächlich Verfahren der Kryptographie kombiniert und eingesetzt. Das im Internet wohl am häufigsten eingesetzt Protokoll zum sicheren Verbindungsaufbau, ist das von der Firma Netscape entwickelte SSL Protokoll.
SSL besteht eigentlich aus zwei getrennten Protokollen. Bei SSL wird durch ein sogenanntes Handschake Protokoll mittels asymmetrischer Verschlüsselung eine Verbindung zur Gegenstation aufgebaut. Steht diese Verbindung einigen sich die zwei Rechner auf ein beiden bekanntes symmetrisches Verschlüsselungsverfahren und tauschen untereinander geeignete Schlüssel für dieses Verfahren aus. Jetzt kommt der zweite Teil von SSL zum Zuge, er baut eine symmetrisch verschlüsselte Verbindung zwischen den beiden Teilnehmern auf und der Datenaustausch kann stattfinden. Bei SSL können beliebige Verschlüsselungsverfahren eingesetzt werden, sie müssen aber beiden Teilnehmern bekannt sein.
Eine weitere Art der Kommunikation bildet im Internet das E-Mail System. Zur Sicherung von E-Mails existieren diverse Programme, die meistens asymmetrische Verschlüsselung, sowie Hashing zur Sicherung der E-Mails einsetzten. Den de facto Standard bildet hier das Programm PGP.

2.2 Authentifizierung:

Authentifizierung kann auf verschiedene Arten verwirklicht werden. Der sich ausweisende besitzt eine Fähigkeit, die außer ihm niemand besitzt. Er besitzt ein einzigartiges Merkmal, wie z.B. biometrische Eigenheiten (Fingerabdruck, Iris) oder aber er beweist die Kenntnis eines nur ihm bekannten Geheimnisses und die ohne das Geheimnis zu verraten.
Hier stellen die asymmetrischen Verschlüsselungsverfahren die benötigten Techniken zur Verfügung. Verschlüsselt eine Person ein Dokument mit ihrem privaten Schlüssel, so kann es mit Hilfe des öffentlichen Schlüssels und nur mit diesem wieder entschlüsselt werden. Somit lässt sich mit Sicherheit feststellen, wer ein Dokument verschlüsselt hat. Ein Nachteil dabei ist, dass das Dokument nicht im Klartext vorliegt und man sich sicher sein muss das ein öffentlicher Schlüssel auch zu der Person gehört, die behauptet das Dokument signiert zu haben. Man kombiniert nun dieses Verfahren mit einem geeigneten Hashingverfahren und erhält dadurch eine digitale Signatur. Es wird der Hashwert des Dokumentes vom Verfasser mit asymmetrischer Verschlüsselung verschlüsselt, und an das Dokument gehängt. Will man nun die Echtheit des Dokumentes überprüfen, muss man nur den Hashwert entschlüsseln und mit dem frisch berechneten Wert vergleichen. Stimmen beide Werte überein, so weiß man, dass das Dokument nicht verändert wurde und kann gleichzeitig feststellen, von wem es signiert wurde. Wie eine solche Signatur erstellt, beziehungsweise wie die öffentlichen

Schlüssel der Personen verwaltet und Zugehörigkeit überprüft werden können regelt in Deutschland das Signaturgesetz SigG.

2.3 Zugangskontrolle:

Ein weiteres sicherheitsrelevantes Thema ist beim E-Commerce die Rechtevergabe beziehungsweise die Zugangskontrolle zu sensiblen Daten. Dies wird meistens durch eine Identifikation mittels Benutzter Name und zugehörigem Passwort realisiert. Am problematischsten sind hierbei nicht die eingesetzten System sonder das Verhalten der Benutzter, die häufig leicht zu erratende Passwörter wählen oder diese unsicher aufbewahren. Aber auch die Systeme besitzen ihre Schwächen. Ein großes Problem ist, das solche System anfällig sind gegen sogenannte Brute Force Angriffe, bei denen systematisch alle, oder sehr häufig verwendete, Passwörter ausprobiert werden. Diesem Angriff kann man sehr leicht begegnen indem man nach mehreren Fehlversuchen ein erneutes Anmelden für eine gewisse Zeit verbietet. Dies wiederum wird häufig ausgenutzt um berechtigte Benutzter gezielt auszusperren (siehe auch Verfügbarkeit).

2.4 Schutz der Daten:

Zum Schutz der Daten werden im E-Commerce im Allgemeinen sichere Verschlüsselungsverfahren verwendet, die sich schon seit Jahren bewährt haben und bis zum heutigen Zeitpunkt als unknackbar gelten. Das Problem dabei ist, das diese Verfahren nicht bewiesenermaßen sicher sind, sonder es bis heute einfach nur noch keiner geschafft hat einen Weg zu finden diese Verfahren zu knacken. Problematisch ist dabei, das immer schnellere Rechner entwickelt werden und mit Hilfe dieser Rechner auch diese Verfahren angegriffen werden können (siehe DES). Eine weiter Schwachstelle sind die eingesetzten Softwarepakete. Das beste Verfahren nützt nichts, wenn es schlecht implementiert wird. So enthielt z.B. die erste Version des SSL Protokolls einen Bug, welcher es erlaubte die erzeugten Schlüssel für die symmetrische Verschlüsselung zu rekonstruieren.
Eine weitere Art der Datensicherung welche immer häufiger zum Einsatz kommt ist, die Steganographie. Dabei werden die Daten einfach in einer großen Anzahl von Daten z.B. einem Bild versteckt ohne das man dies den Daten ansehen könnte. Diese Art der Datensicherung ist leider für E-Commerce nur bedingt geeignet, denn wer verschickt den schon Bilder oder Musikdateien an seinen Buchladen?!

2.5 Unveränderbarkeit:

Wie bereits erwähnt kann Verändern der Daten nicht effektiv verhindert werden, weshalb man zumindest versucht Veränderungen mit Sicherheit zu erkennen. Hierzu kommt meist eine Kombination aus Hashverfahren, Verschlüsselung sowie Signaturen zum Einsatz. Die Unveränderbarkeit spielt vor allem im E-Commerce eine sehr bedeutende Rolle, da Kunde und Händler sich stets auf die Richtigkeit eines Auftrags beziehungsweise eines Angebotes verlassen könne müssen. Ein weiteres Problem in diesem Zusammenhang ist die Aktualität. Es darf z.B. nicht möglich sein eine abgefangene Bestellung zu kopieren und zu einem späteren Zeitpunkt erneut an den Händler zu schicken. Dazu muss jede Nachricht mit einer Zeitmarke bzw. einem Gültigkeitszeitraum versehen werden. (Siehe auch elektronische Zahlungssysteme).

2.6 Verfügbarkeit:

Im weiteren Zusammenhang mit der Sicherheit von E-Commerce Systemen steht auch deren Verfügbarkeit, das heißt das die Dienste eines E-Commerce Unternehmens ihren Kunden zu jeder Zeit zur Verfügung stehen müssen und eine Ausfallsicherheit gewährleistet ist. Gerade in diesem Bereich gibt es aber bei den Serviceunternehmen häufig Defizite. So wurden im Laufe des Jahres 1999 mehrere E-Commerce Unternehmen durch gezielte Denial Of Service Angriffe gestört. Dies ist vor allem für zeitkritische Geschäfte gefährlich wie z.B. Online Brokerage Anbieter. Doch dies soll nur am Rande erwähnt werden, weil dadurch nicht direkt eine Gefahr für die Daten der Kunden entsteht.

3. Elektronische Zahlungssysteme:

Hier kurz auf die Funktionsweise von Elektronischen Zahlungssystemen eingegangen werden. Besonderes Augenmerk wird dabei auf deren Sicherheit gelegt. Um das ganze zu komplettieren wird hierbei auch speziell auf Homebankingsysteme eingegangen, die eine eigene Art des E-Commerce bilden.

3.1 Homebanking:

Homebanking bildet bis zum heutigen Tage die am häufigsten eingesetzte Form der elektronischen Zahlungssysteme, wobei hierbei vielmehr die Verwaltung der eigenen Finanzen im Fordergrund steht als das Bezahlen von Dienstleistung oder Waren auf elektronischem Wege. Die heutigen Systemen beruhen dabei meist auf reinen Softwarelösungen, die mit PIN und TAN Authentifizierung arbeiten, aber auch Lösungen mit Hardware Komponenten sind im Einsatz. In Deutschland wurde jetzt von Zentralen Kreditausschuss der branchenübergreifende Homebankingstandard HBCI entwickelt. Der HBCI Standard sieht dabei alle Arten der Datensicherung sowie der Datenverifizierung vor. HBCI legt dabei nur eine gemeinsame Schnittstelle fest, die eine Banken unabhängige Auftragsabwicklung ermöglicht und dabei strenge Sicherheitsvorgaben macht. HBCI ist ein offener Standard, der von allen modernen Sicherungsverfahren gebrauch macht und deshalb als sehr sicher gilt.

3.2 Allgemeine Probleme:

Bei der Entwicklung von elektronischen Zahlungssystemen kristallisierten sich einige schwerwiegende Problem heraus, die es zu lösen gilt. So muss das elektronische Geld sehr gut gegen Manipulation jeglicher Art geschützt werden, da Manipulationen von digitalen Daten ungleich leichter sind wie bei echtem Geld. Geld darf nicht duplizierbar sein, das heißt jede Geldeinheit muss eine eigenen Identität besitzen, was bei Hartgeld nicht der Fall ist. Diese Tatsche verlangt einen immensen Verwaltungsaufwand, da für jeden Pfennig und jedes Markstück eine eindeutige Identität erschaffen und gespeichert werden muss um Kopien erkennen zu können. Dies wirft ein weiteres Problem auf, wenn bei der Übertragung von Geld ein Fehler auftritt geht es einfach verloren und löst sich in Luft auf, es sie denn man hat eine KOPIE die man erneut senden kann was aber wieder zu oben genannten Problem führt.
Ein weiteres Problem ist die Echtheit von Geld. Wie verhindere ich, dass sich die Leute ihr Geld einfach selber machen, bzw. gar keine Berechtigung haben dieses gültige Zahlungsmittels in Anspruch zu nehmen. Dies betrifft vor allem die Kreditkartensysteme.

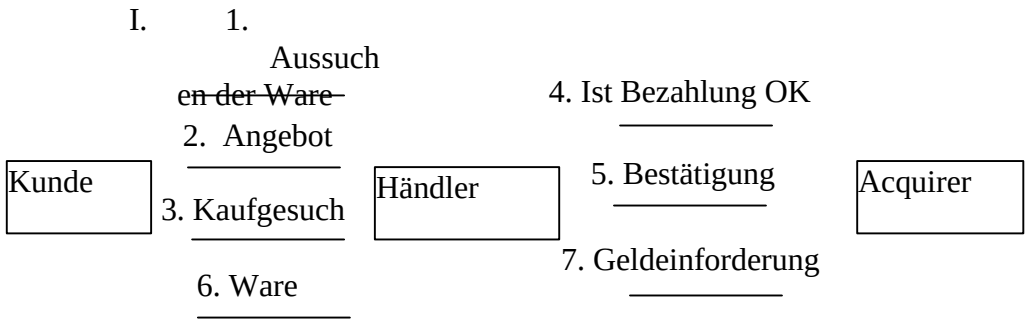
Des weiteren bringt jedes entwickelte System noch eigene Schwächen und Probleme mit sich, die im folgenden besprochen werden.

3.3 Verschiedene Arten von Zahlungssystemen:

Bei den hier vorgestellten Systemen wir zwischen Kreditkartensystem und sogenannten Micropayment Systemen unterschieden. Letztere ermöglichen es auch kleinere Beträge zu begleichen, sie stellen im wahrsten Sinne des Wortes eine Art digitales Geld dar.
Die Kreditkartensysteme gibt es in unterschiedlichsten Implementierungen sowie abgewandelten Formen, die auf Schecksystemen oder Überweisungen beruhen, sie basieren jedoch alle auf ähnlichen Ansätzen.

3.4 Kreditkartensysteme:

Kreditkartensystem haben alle gemeinsam, das sie die eigentlichen Zahlungsvorgänge über eine Kreditkarte abwickeln. Dabei bildet die Authentifizierung das größte Problem dieser System. Das Problem hierbei ist, das Kreditkartennummern nicht an eine bestimmte Person gebunden sind. Die Nummer lässt sich zwar durch ein mathematisches Verfahren auf Gültigkeit prüfen, nicht aber ob diese Kreditkartennummer zu der Person gehört, die Sie benutzt. Hinzu kommt, das sich gültige Kreditkartennummern nach belieben selbst erstellen lassen. Auch ist problematisch, dass man diese Nummer an den Händler übergeben muss und man diesem vielleicht nicht immer ganz trauen kann, ob er mit dieser Nummer keinen Missbrauch treibt. Genau bei diesem Problem setzten die Kreditkartensysteme an. Als Beispiel soll hier das SET Protokoll betrachtet werden.

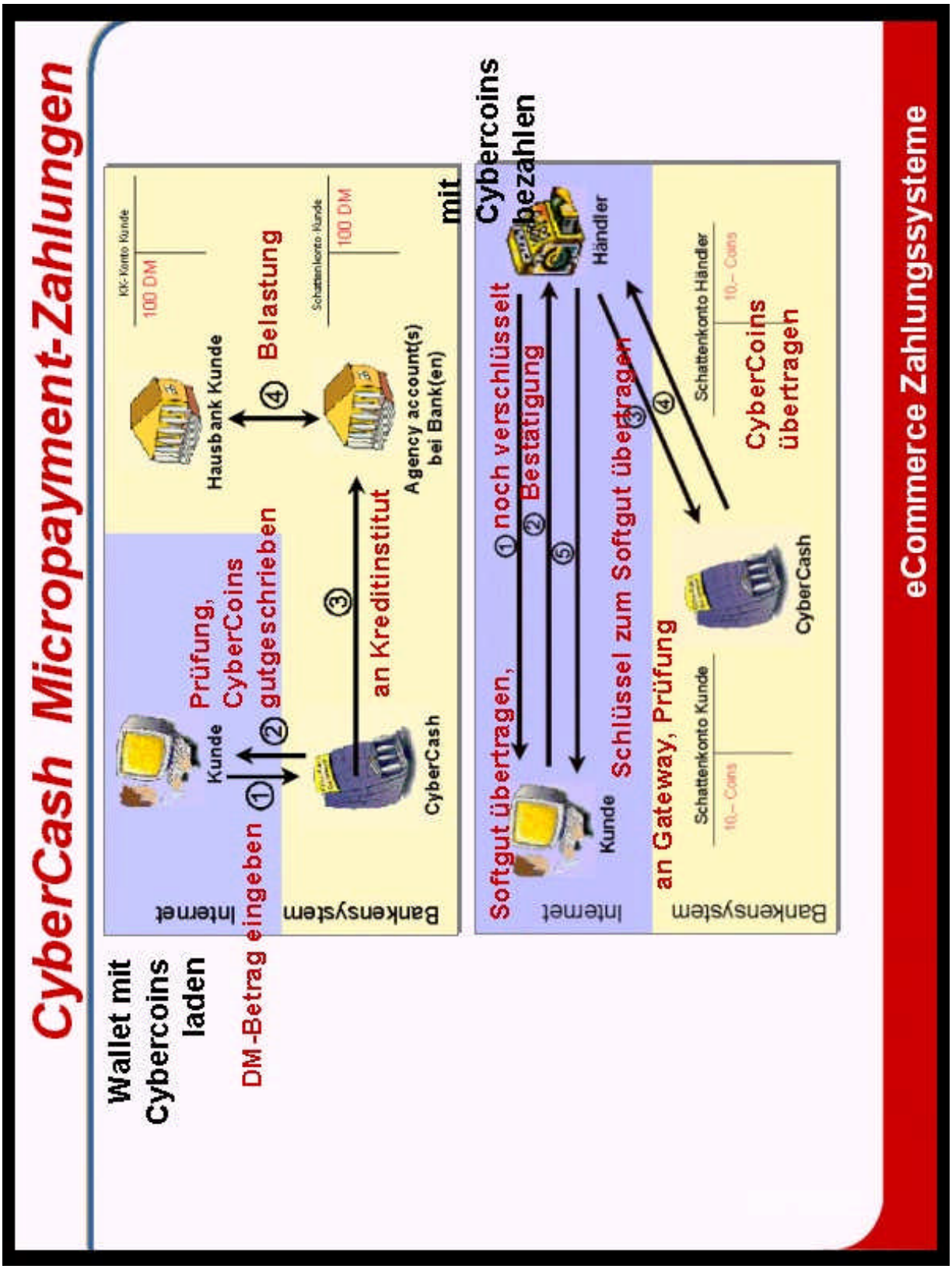


Das SET Protokoll wurde von den führenden Kreditkartenherstellern entwickelt und wird sich schon alleine deswegen zum Standard entwickeln. Bei SET wird eine Kreditkartentransaktion die erfolgen soll von einem sogenannten Acquirer, einer von den Kreditkartenherstellern zertifizierten Stelle überprüft und gegebenenfalls bestätigt. Dies läuft folgender maßen der Händler fordert vom Kunden eine Bezahlung an. Der Kunde übergibt dem Händler seine Kreditkartennummer sowie die Daten zur Person und zur eigentlichen Bestellung in verschlüsselter Form, dazu wird ein asymmetrisches Verfahren mit dem öffentlichen Schlüssel des Acquirers verwendet. Der Händler reicht diese Daten zusammen mit seiner Version der Bestellungsdaten an den Acquirer weiter. Der Acquirer entschlüsselt die Daten des Kunden und vergleicht sie mit den Bestelldaten des Händlers. Stimmen diese überein und ist der Kunde berechtigt mit der Kreditkartennummer eine Zahlung durchzuführen erhält der Händler ein OK und liefert die Ware an den Kunden. Sollte der Händler versuchen den Kunden zu betrügen wird er aus dem SET System ausgeschlossen. Der Vorteil dieses

Verfahrens ist, das die Kreditkartendaten des Kunden geheim bleiben und der Händler eine Sicherheit für die Zahlung hat. Nachteile sind, das dieses System sich nicht für kleine Beträge rentiert und das diese in der Theorie gute System in der Praxis eine Schwäche hat. In der Praxis überprüft der Acquirer zwar die Gültigkeit der Kreditkarte aber nicht die Zugehörigkeit zu der Person, wobei wir wieder bei dem Problem der künstlich erstellten Kreditkarten wären.

3.5 Micropayment Systeme:

Unter Micropayment Systemen versteht man Systeme, die Versuchen Geld digital abzubilden. Dazu haben sich gerade in der letzten Zeit einige Systeme entwickelt, die aber allesamt noch in der Entwicklung oder Testphase stecken oder aber sich noch nicht im praktischen Einsatz bewährt haben. Das macht es schwierig die Sicherheit dieser Systeme ab zuschätzten. Diese Systeme sind dabei vor allem für die Begleichung von kleinen Beträgen sinnvoll, wo sich der Einsatz von Kreditkartensystemen nicht lohnt. Micropayment Systeme müssen dabei aber mit einer ganzen Anzahl von Problemen kämpfen. Das größte Problem ist hier sicher der Schutz vor Dubletten. Um dies zu gewährleisten müssen die Geldeinheiten entweder ungemein schwer zu Erstellen sowie zu Kopieren sein, oder aber eindeutig erkennbar sein. Alle eingesetzten Mittel zum Schutz dieser Systemen verlangen einen sehr großen Aufwand was häufig dazu führt das diese System nicht rentabel sind. Folgendes Bild soll einen Überblick über ein Micropayment System geben.



Ein weiteres Problem bildet der Geldfluss. Die meisten Systeme sind nur für eine Dreiecksbeziehung zwischen Kunde, Händler und Bank geeignet d.h. die Weitergabe der Geldeinheiten an weitere Zwischenpersonen geht entweder nicht oder aber stellt ein

Sicherheitsproblem dar. Folgendes Beispiele soll dies verdeutlichen. Ein Kunde kauft etwas bei Händler A. Dieser Händler wiederum gibt das Geld an Händler B weiter und erhält dafür Waren. Händler A hat aber eine Kopie der Geldeinheiten erstellt und löst diese jetzt schnell bei der Bank ein. Der Kunde kauf für das gleiche Geld etwas bei Händler C, auch der Kunde hat eine Kopie des Geldes erstellt, und dieser will das Geld jetzt bei seiner Bank einlösen ebenso Händler B. Die Bank stellt fest, das dieses Geld schon verwendet wurde und deckt den Betrug auf, doch wer hat das Geld kopiert? Der Kunde oder Händler A, oder Händler B. Die Bank müsste sich merken wer welche Geldeinheit einlöst und auch dann könnte sie nicht sicher sein ob das Geld nicht von anderen auch schon vorher kopiert wurde.
Das Problem liegt hierbei darin, das nur die Bank, die das Geld erstellt und eintauscht einen Betrug feststellen kann, von wem der Betrug aber begangen wurde kann im Nachhinein nicht nachvollzogen werden. Zur Zeit sind entstehen gerade hier viele neue Systeme und manche sind auch schon seit geringer Zeit im Einsatz. erwähnenswert sind die Systeme CyberCoin, der Firma Cybercash, PayWord von Ron Rivest und Adi Shamir sowie die Verfahren Millicent und MicroMint.

Fazit:

Datensicherheit ist im Bereich des E-Commerce von entscheidender Rolle. Einer der Hauptgründe dafür das der erwartete Boom für das E-Business bis jetzt ausgeblieben ist liegt sicher auch daran, das die Menschen bis jetzt wenig Vertrauen in die existierenden System haben. Mit unter zu Recht, den viele System sind zu neu und unausgereift um als wirklich sicher gelten zu können. Gerade im Bereiche der elektronischen Zahlungssysteme wurde bis jetzt nur Pioneerarbeit geleistet und dies häufig auch nur mit schlechten Implementierungen. Häufig ist es nicht Ziel ein funktionierendes System zu schaffen, sonder nur die Entwicklung einer Idee um ein Paten auf sie zu erhalten. Der E-Commerce Sektor braucht allgemein anerkannte Standards wie SSL, HBCI und SET um einen sicheren Standard aufzubauen und Vertrauen bei den Kunden zu gewinnen. Im allgemeinen sind alle nötigen Vorraussetzungen gegeben um E-Commerce sicher zu machen. Die Sicherheitsprobleme entstehen häufig durch schlechte Umsetzungen dieser Techniken aus Zeit oder Kostengründen. Wirklich sichere System werden sich aber im Lauf der Zeit durchsetzten und der Welt die Tore zum E-Commerce aufstoßen.

Ein weiterer Aspekt der zu betrachtet werden will ist der Datenschutz im E-Commerce, denn häufig stören sich diese beiden Bereiche auch gegenseitig und es muss ein Kompromiss gefunden werden. Wie ist es zum Beispiel möglich absolut anonyme Zahlungssysteme zu entwickeln, die gleichzeitig eine Aufklärung von Missbrauch durch eine Person ermöglichen. Eine kurze Abhandlung zu diesem Thema entstand im Rahmen der Vorlesung Datensicherheit und Datenschutz durch Sergej Klatt.

Literaturnachweis:

Bücher:

E-Commerce und Hackerschutz *Einführung Datensicherheit im E-Commerce*

Gunter Lepschies Vieweg, Verlag 1999

Applied Cryptography *Standardwerk zum Thema Kryptographie*
Bruce Schneier John, Wiley & Sons

Sicherheit im Internet *Allgemeines zum Thema Sicherheit im Internet*
Othmar Kyas MITP Verlag 1998

Sicherheitsaspekte bei Elektronic Commerce *Gutes Buch zum Thema E-Commerce*
Band 10, BSI 1999

Ein paar ausgewählte Internetquellen:

www.bsi.de	Alles zum Thema Datensicherheit Standards und Gesetzt
www.rsa.com	Entwickler der meist benutzten Verschlüsselungstechniken

Micropayment:

www.cybercash.de	Anbieter von Cybercash und CyberCoin
www.millicent.de	Informationen über das MilliCent E-Payment System

Viele weitere interessante Text können in den gängigen Webkatalogen gefunden werden:

www.yahoo.de
www.dino-online.de

