Skriptum zur Vorlesung

DATENSCHUTZ UND DATENSICHERHEIT

Kryptographische Protokolle für elektronische Transaktionen

Kryptographische Infrastruktur

Wintersemester 2001/2002

Vortragender:

Dr. Jörg Pflüger

Kryptographische Protokolle für elektronische Transaktionen

Weitgehend nach der Vorlesung »Datenschutz und Datensicherheit« von Klaus Pommerening, http://www.uni-mainz.de/ Dort finden sich auch viele Literaturangaben.

1. Starke Authentisierung

Starke Authentisierung ist eine weitere Anwendung von digitalen Signaturen. Es handelt sich um einen erheblich besseren Erkennungsdialog als die allgemein gebräuchliche Methode, einen Zugang durch Paßwörter zu schützen.

Herkömmlicher Erkennungsdialog mit Paßwortabfrage:

- Benutzerin meldet sich an,
- wird nach ihrem Paßwort gefragt,
- überträgt dieses (oder gibt es ein) und
- wird zum System zugelassen, falls es korrekt ist.

Die Überprüfung geschieht meist mit einer Einweg-Funktion, wobei das Bild des Paßwortes mit den Einträgen in einer (geschützten) Paßwortdatei verglichen wird.

Gefährdungen von Paßwörtern:

- Nachlässigkeit der Besitzer
- Social Engineering
- ungenügende Schutzvorkehrungen des Systems
- Abhören von Leitungen, Bildschirmen etc.
- Paßwortfallen, Trojanische Pferde
- Systematisches Durchprobieren (mit Wörterbüchern)

Auch wenn der Paßwortschutz eine veraltete Technik darstellt, ist damit immerhin ein Hinweis gegeben, daß der Zugang nur für ausdrücklich Befugte gestattet ist und hat somit strafrechtliche Relevanz.

Analogie: Gleich welche Qualität ein Schloß hat, ist das Aufbrechen einer abgeschlossenen Tür ein Einbruch.

Starke Authentisierung:

Die starke Authentisierung ist ein abhörsicherer Erkennungsdialog, der auf einem Challenge-Response-Mechanismus beruht:

- Benutzerin Alice verwendet ein asymmetrisches Schlüsselpaar (v,d).
- Sie sendet dem System eine Anmeldung mit ihrer Identität und öffentlichem v.
- System erzeugt Zufallsnachricht m (challenge) und sendet diese an Alice.
- Alice signiert m mit ihrem geheimen d und sendet die Signatur s (response) zurück.
- Das System prüft, ob sich aus s mit Alice v wieder m ergibt.

Dadurch ist eine zweifelsfreie Identifizierung gegeben, was aber wieder voraussetzt, daß der öffentliche Schlüssel durch ein Zertifkat abgesichert ist, da sonst ein Betrug durch eine Masquerade möglich ist.

Abhören der Leitung und Wiederholen der Eingabe (»replay attack«) sind wirkungslos.

Man kann das Verfahren durch gegenseitige Authentisierung verbessern, indem man verlangt, daß das Zielsystem die Signatur s signiert und an Alice schickt.

Techniken des Social Engineering

Hauptsächliche Anwendungsbereiche:

- Erschleichen von Paßwörtern
- Installation von Trojanischen Pferden.

Social Engineering besteht darin, Nutzer zu 'übertölpeln', indem ihr Vertrauen oder ihre Interessen ausgenutzt werden, z.B.

- dringender Anruf des 'Systemadministrators',
- Behauptung, daß im Attachment einer Mail ein Patch oder Upgrade enthalten ist,
- Vortäuschen eines Spiels, um Anwender zur Ausführung eines Programms zu verführen,
- Email so verfälschen, daß sie von einem Bekannten zu kommen scheint.
- Schädling in harmloser oder vertrauter Form verpacken (z.B. bekanntes Icon oder falscher Suffix)
- Bestechung, Erpressung

2. Blinde Unterschrift

Was soll die blinde Unterschrift leisten?

a) Unterschrift:

Ein Dokument wird unterschrieben, ohne daß der Unterschreibende dessen Inhalt erkennen kann. Die Unterschrift bestätigt also nicht den Inhalt des Dokuments, sondern die Tatsache der Vorlage durch eine bestimmte Person zu einem bestimmten Zeitpunkt.

b) Prüfung:

Dokument + Unterschrift werden vorgelegt. Der Prüfende kann erkennen, ob die Unterschrift

1. zum Dokument gehört und
2. rechtmäßig erlangt wurde.

c) Anonymität (optional):

Der Unterschreibende kann, wenn er Dokument + Unterschrift später wiedersieht, dieses dem Besitzer nicht zuordnen (also auch den Unterschriftvorgang nicht rekonstruieren).

Veranschaulichung einer blinden Unterschrift:

Das Dokument wird in einen Umschlag gesteckt, der innen mit Durchschlagpapier beschichtet ist. Die Unterschrift erfolgt außen auf dem Umschlag und wird auf das Dokument übertragen, das später wieder aus dem Umschlag geholt wird.

Beispielszenario: Testament

Ein Notar bescheinigt durch blinde Unterschrift die Echtheit eines Testaments, ohne dessen Inhalt zur Kenntnis zu nehmen.
Nach dem Ableben des Erblassers wird dem Notar das Testament vorgelegt. Jetzt nimmt er den Inhalt zur Kenntnis und regelt die Erbschaft.

Allgemeines Szenario der blinden Unterschrift

Beteiligte:

A (Alice) Besitzerin des Dokuments
B (Bob) Prüfer des Dokuments (»Öffentlichkeit«)
N (Nancy) Unterzeichner (»Notar«) (B = N ist möglich)

Mögliche Sicherheitsansprüche: Geheimhaltung des Dokumenteninhalts oder der Besitzerin

vor N beim Unterzeichnungsvorgang,
vor B beim Prüfvorgang,
vor N beim Prüfvorgang.

Signaturparameter: Alle Informationen über das Dokument, die N bei der Unterzeichnung sieht.

Typen der blinden Unterschrift:

In allen Fällen kann N das Dokument beim Unterzeichnungsvorgang nicht lesen.

1. *Verdeckte Unterschrift:*

   N kann das Dokument später wiedererkennen und lesen (aufgrund der Signaturparameter), ohne daß die Unterschrift mit vorgelegt wird.

   Daher kann N es auch der Besitzerin A zuordnen.

2. *Schwach blinde Unterschrift:*

   N kann das Dokument wiedererkennen, aber nur, wenn es ihr zusammen mit der Unterschrift vorgelegt wird.

3. *Stark blinde Unterschrift:*

   Auch wenn N Dokument + Unterschrift wiedersieht, kann sie es A nicht zuordnen.

(Die Klassifikation ist in der Literatur uneinheitlich.)

Mögliche Anwendungen:

- elektronisches Geld (rechtskräftig, aber anonym),
- beglaubigte Pseudonyme,
- anonyme Berechtigungsausweise (Berechtigung nachweisbar ohne Preisgabe der Identität, anonymisierte Zertifikate),
- geheime, von Dritten blind beglaubigte Verträge,
- elektronische Wahlen (unter Wahrung des Wahlgeheimnisses).
- und vieles mehr

Sinn: Rechtssicherheit trotz Anonymität!

Achtung! Ein Schlüssel, der für blinde Unterschriften verwendet wird, sollte für nichts anderes verwendet werden. Sonst kann es passieren, daß man etwas rechtsgültig unterschreibt, was man gar nicht wollte, z. B. einen Schuldschein.

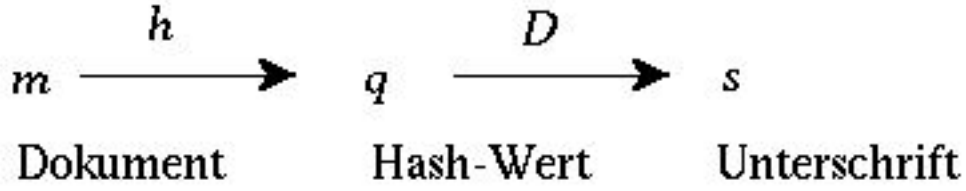
Blinde Unterschriften sind nur in ganz bestimmten Szenarien sinnvoll, die gut durchdacht sein müssen.

Konstruktion einer verdeckten Unterschrift

Voraussetzung:

- eine kryptographisch sichere Hash-Funktion h, die öffentlich bekannt ist,
- eine Signatur-Funktion, deren Parameter Geheimnis von N sind.

Verfahren: (Signaturparameter: q, s)



Eigenschaften:

- Wenn N das Dokument m sieht (auch ohne Signatur), kann sie es wiedererkennen, da sie q gesehen hat, folglich h(m) berechnen und mit q vergleichen kann.

Also handelt es sich um eine verdeckte Unterschrift.

- Eine Fälschung ist nicht möglich, denn sonst müßte A zu gegebenem s und q = V(s) ein m so wählen können, daß q = h(m), was im Widerspruch zur Sicherheit des Hash-Funktion stünde.

Erst recht ist das Finden eines geeigneten s zu gegebenem m unmöglich.

Konstruktion einer stark blinden Unterschrift

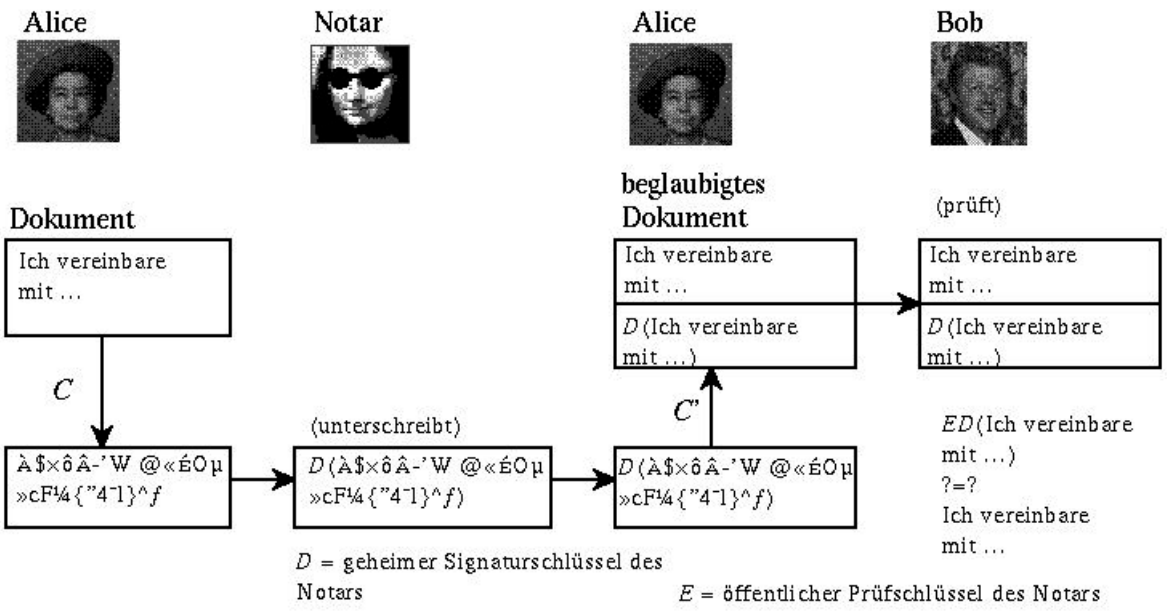
Prinzip:

- Das Dokument m wird von A vor der Unterschrift in eine unleserliche Gestalt C(m) transformiert, z. B. unter Verwendung eines Zufallsschlüssels. Dies wird auch »Camouflage« genannt.
- Dann wird die Camouflage von N unterschrieben: D(C(m)).
- Nach der Unterschrift wird es von A zurücktransformiert: C'(D(C(m))) ?=? D(m).

Damit das funktioniert, muß die Rücktransformation C' aus C (und bekannten Parametern) leicht bestimmbar sein.

C muß von A geheim gehalten werden!

Ablauf einer stark blinden Unterschrift:



Realisierung mit RSA:

N hat RSA-Schlüssel mit öffentlichem Teil (n,v) und geheimem Teil d.

Erzeugung:

Alice, die das Dokument m unterschreiben lassen will

1. wählt eine große Zahl c (zur Camouflage) zufällig,
2. bildet das camouflierte Dokument $M = c^v\ m \bmod n$, (Verschiebeschiffre, perfekt sicher)
3. gibt M an N.

N gibt unterschriebene Camouflage $t = M^d \bmod n$ an Alice zurück.

A entfernt die Camouflage: $s = t\ c^{-1} \bmod n$.

Es gilt: $s = Md\ c^{-1} = c^{vd}\ m^d\ c\text{-}1 = m^d \bmod n$, und das unterschriebene Dokument ist (m,s).

Prüfung:

Mit dem öffentlichen Schlüssel v von N muß gelten: $s^v \bmod n = m$.

Signaturparameter: M, t.

Eigenschaften:

N kann das Dokument nicht wiedererkennen oder der Besitzerin zuordnen, da sie nur M gesehen hat.

Also handelt es sich um eine stark blinde Unterschrift.

Literatur:

David Chaum: Security without identification: Transaction systems to make Big Brother obsolete. Communications of the ACM 28 (1985), 1030 - 1044.
http://www.digicash.com/news/archive/bigbro.html

Birgit Pfitzmann, Michael Waidner, Andreas Pfitzmann: Rechtssicherheit trotz Anonymität in offenen digitalen Systemen. DuD 14 (1990), 243 - 253, 305 - 315.
http://www.semper.org/sirene/publ/PWP_90anonyZsys.ps.gz

3. Pseudonyme

Pseudonyme sind kryptographische Protokolle zur Wahrung der Anonymität:

- mit kontrolliertem Datenabgleich
- unter Wahrung der informationellen Selbstbestimmung.

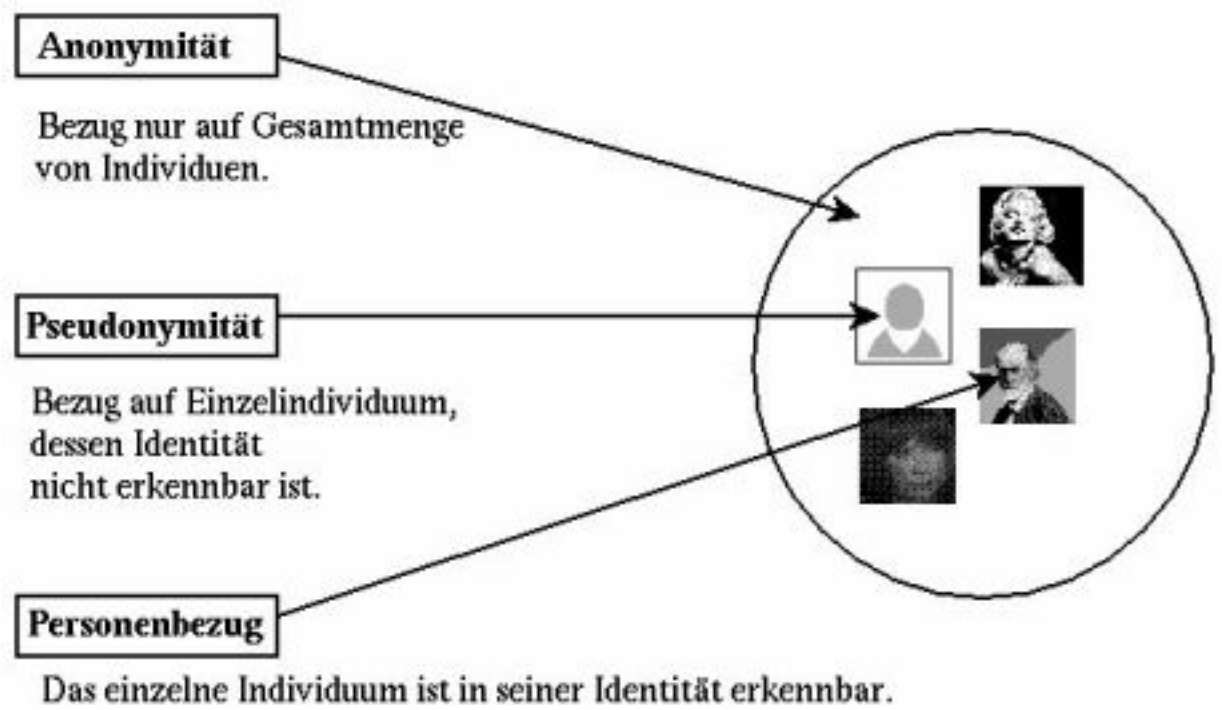
Exemplarische Problembereiche:

- Spuren im Netz, z. B. beim Profiling beim eCommerce.
- Auswertung medizinischer Daten (Forschung, Qualitätssicherung)

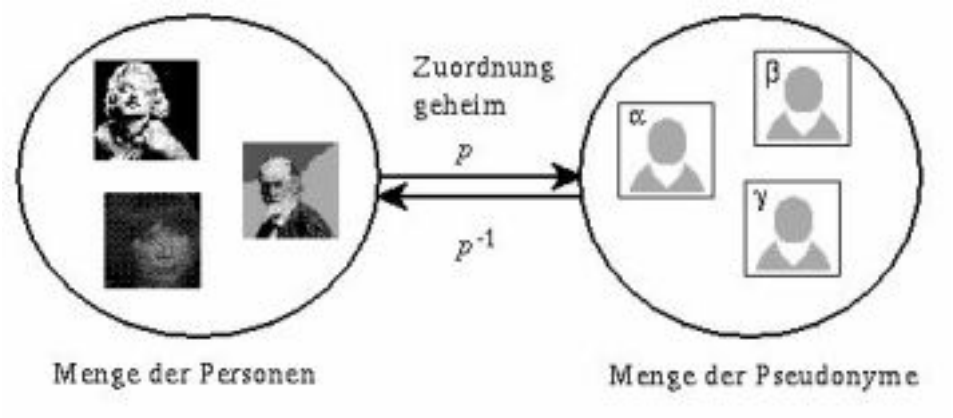
Pseudonyme verschleiern den Personenbezug so, daß faktische Anonymität entsteht, ohne die Verwendung der Daten zu Forschungszwecken oder die Rechtssicherheit von geschäftlichen Transaktionen zu behindern. Der Personenbezug ist zur Erfüllung der Zweckbestimmung der Daten sehr oft nicht notwendig, seine Beibehaltung somit unnötig (oder gesetzwidrig).

Pseudonyme im täglichen Leben: bei Schriftstellern, Schauspielern oder Spionen als 'Decknamen'.

Drei Bezüge zwischen öffentlicher Äußerung und Urheber:

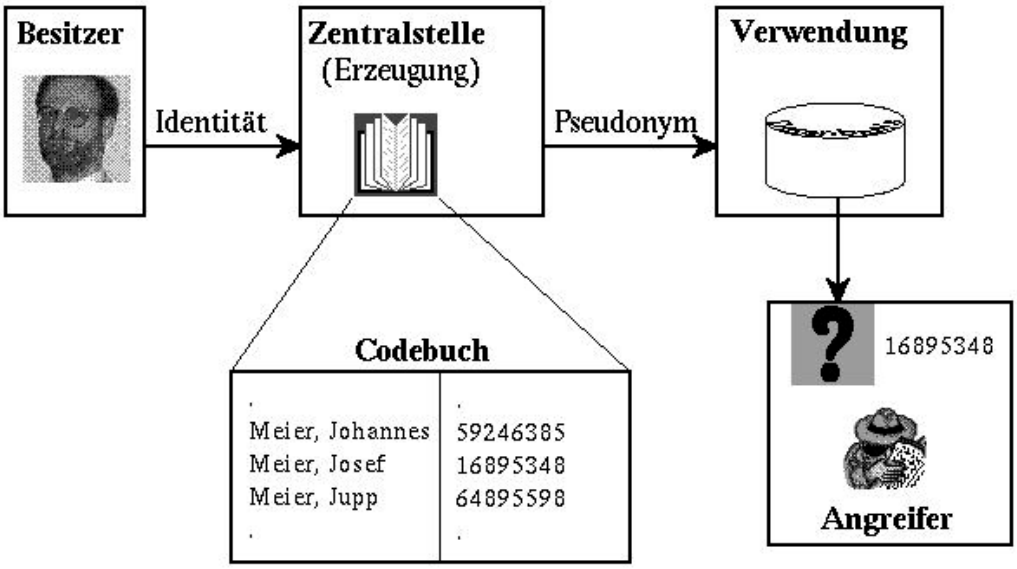


Pseudonyme sind geheime Zuordnungen von Zeichenketten zu Personen.



Die Zuordnung ist nicht notwendig bijektiv. Eine Person kann mehrere Pseudonyme oder natürlich auch gar kein Pseudonym haben.

1. Realisierung von Pseudonymen (Referenzlistenmodell (»Codebuch«)):



Nachteil: Die zentrale Referenzliste ist ein riesiger Angriffspunkt.

2. Realisierung von Pseudonymen (kryptographische Lösung):

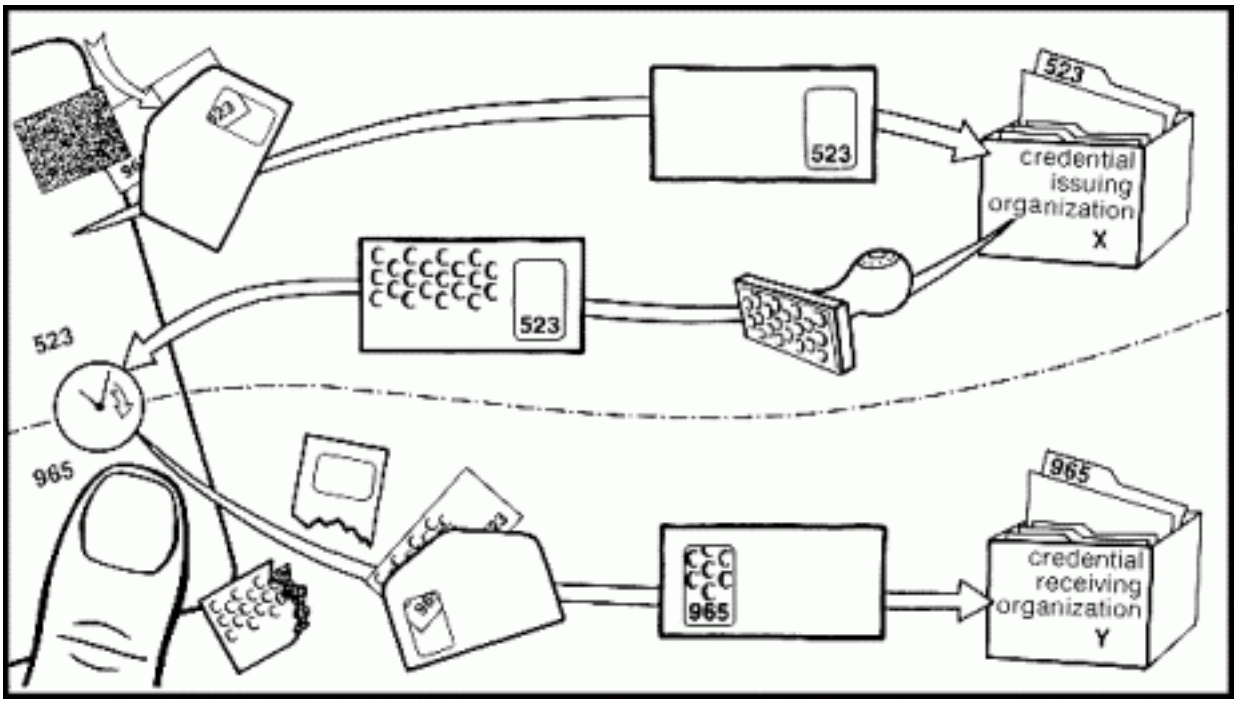
Die kryptographische Realisierung von Pseudonymen basiert auf der blinden Unterschrift.

Anforderungen:

1. Keine zentrale Referenzliste.
2. Zentralstelle soll nur als »Certification Authority« (Nancy) mitwirken.
3. Der Pseudonyminhaber verwaltet sein Pseudonym selbst.
4. Zusammenführung der Daten bleibt trotz Pseudonymen erhalten.
5. Transaktionen unter Pseudonym können beweissicher gestaltet werden.

Je nach Ausgestaltung des Protokolls werden diese Anforderungen mehr oder weniger erfüllt.

Eine Erweiterung der Kohlepapier-Metapher auf Fenster-Umschläge veranschaulicht, wie man mit verschiedenen Pseudonymen zwischen verschiedenen Organisationen verkehren kann und trotzdem die richtigen Beglaubigungen (»credentials«) bekommen kann. Rechtssicherheit trotz Pseudonymität!



Im Idealfall sollte, gemäß der Idee der informationellen Selbstbestimmung, nur der Besitzer seine Pseudonyme lüften oder verschiedene Pseudonyme zusammenführen können. Das ist allerdings nicht bei allen Anwendungen sinnvoll, z.B. im Falle krimineller Aktivitäten.

Anwendungsfelder

- Krebsregister
- anonyme Krankenkassenabrechnung
- anonymes elektronisches Rezept
- anonyme Berechtigungsausweise (z. B. Fahrkarten ohne
- Bewegungsprofil)
- anonyme Verträge
- elektronisches Geld
- elektronische Wahlen

Anwendungsbeispiel 1: Krebsregister

Hintergrund:

- Meldung aller Krebsfälle an zentrale Register Zweck: Epidemiologische Erforschung der Krebserkrankungen (Ursachen, Auswirkungen von Vorsorge- und Therapiemaßnahmen).
- Bundes- und Landeskrebsregistergesetze.

Anforderungen:

1. Das Register muß in der Lage sein, durch Abgleich Mehrfachmeldungen zu erkennen (»record linkage«).
2. Die Abgleichsprozedur soll Synonym- und Homonym-Fehlerraten minimieren.
3. Die Register der verschiedenen Bundesländer sollen ihre Bestände abgleichen können.

4. Unter kontrollierten Umständen soll die Aufdeckung von Pseudonymen möglich sein.
5. Der Besitzer soll sein eigenes Pseudonym nicht aufdecken können. (Aufklärung durch Arzt, nicht durch Registerabfrage.)

Realisierung:

- Aufteilung des Krebsregisters in Vertrauensstelle und Registerstelle:
  - Vertrauensstelle erzeugt Pseudonyme.
  - Registerstelle speichert nur pseudonymisierte Daten.
- Pseudonyme zweiteilig:
  1. Teil : deterministisch mit Hilfe von Hash-Funktion (schlüsselabhängig). Aufteilung in Kontrollnummern, um Fehlerrate zu minimieren.
  2. Teil: durch asymmetrische Verschlüsselung der ID, Rückschlüssel bei externer Aufsichtsstelle.

  Der erste Teil des Pseudonyms ermöglicht die Zusammenführung von Mehrfachmeldungen. Der zweite Teil des Pseudonyms ermöglicht Identifizierung des Patienten unter Kontrolle der Aufsichtsstelle.

- Länderübergreifender Abgleich über gemeinsamen Einmalschlüssel.
- Pseudonyme werden nicht öffentlich zugänglich gemacht.

Anwendungsbeispiel 2: Krankenkassenabrechnung

Anforderungen:

1. Die Krankenkassen müssen bei der Abrechnung der Behandlung zweifelsfrei erkennen, daß die Leistungen für eines ihrer Mitglieder erbracht wurden.
2. Die Krankenkassen sollen keine personenbezogenen Krankheitsgeschichten sammeln können.
3. Die Krankenkassen sollen ihre Risiken kalkulieren können

   durch einzelfallbezogene Auswertung von Krankheitsverläufen,
   durch Erkennen der Kosten für bestimmte Krankheitsbilder.

Vorgeschlagene Realisierung: (bisher an politischen Widerständen gescheitert!)

Pseudonym-Erzeugung

- Die Patientin erhält Versichertenkarte von Krankenkasse.
- Die Patientin wählt zu Hause (oder beim Arzt) Pseudonym und camoufliert es.
- Die Krankenkasse unterschreibt das Pseudonym auf der Karte blind.
- Die Patientin entfernt die Camouflage.

(Das Pseudonym muß eine vorgeschriebene Struktur haben, z. B. 20-stellige Zahl, als ASCII-Zeichen geschrieben. Sonst Fälschung möglich durch Anwendung des öffentlichen Prüfschlüssels v.)

Pseudonym-Verwendung

- Die Patientin legt Versichertenkarte dem Arzt vor und schaltet das Pseudonym durch PIN-Eingabe frei.
- Der Arzt übernimmt das Pseudonym (als Versichertennummer), prüft es auf Gültigkeit und verwendet es zur Abrechnung.
- Die Krankenkasse erkennt das Pseudonym als echt, kann mit dem Arzt abrechnen und die Daten der Patientin zusammenführen.

Anwendungsbeispiel 3: elektronisches Rezept

Das elektronische Rezept wird

- vom Arzt elektronisch signiert,

- in die Chipkarte des Patienten eingetragen,
- in der Apotheke geprüft und bearbeitet,
- an die Krankenkasse übermittelt,
- vollelektronisch abgerechnet.

Das elektronische Rezept wird pseudonymisiert:

- Im Rezeptkopf steht statt Name, Adresse und Mitgliedsnummer ein Pseudonym des Patienten.
- Auch der Arzt kann durch ein Pseudonym repräsentiert werden.
- Kostenabrechnung und Auswertungen bleiben möglich, z. B.:
    - ob das Rezept für ein Mitglied der betreffenden Krankenkasseerstellt wurde und gewisse Merkmale (Geschlecht, Geburtsjahr),
    - ob das Rezept von einem zugelassenen Kassenarzt ausgestellt wurde, einschließlich Facharzt-Richtung,
    - welche Rezepte in einem Zeitraum für eine Person ausgestellt wurden,
    - wie oft ein Arzt welche Medikamente verordnet.

In begründeten Fällen (gesetzlich geregelt) ist eine Aufhebung der Pseudonyme möglich mit spezieller Re-Identifizierungskarte (oder Zusammenwirken zweier Karten).

Zusammenfassung

Durch die Einführung von Pseudonymen läßt sich in vielen Anwendungsbereichen der Informationstechnik ein tragbarer Kompromiß zwischen dem informationellen Selbstbestimmungsrecht der Bürger und dem Datenhunger von Forschung und Gesellschaftspolitik sowie dem Anspruch auf Rechtssicherheit im Geschäftsverkehr finden.

Chipkarten (als Ausweiskarten aller Art) werden durch die Verwendung von Pseudonymen von einem Instrument der informationellen Entblößung zu einem Instrument der informationellen Selbstbestimmung.

Kryptographische Pseudonyme stellen eine Grundtechnik des praktischen Datenschutzes dar. Sie sollten, wo immer möglich, eingesetzt werden.

Allerdings steht ihrer Realisierung oft der politische Wille entgegen.

Literatur:

David Chaum: Security without identification: Transaction systems to make Big Brother obsolete. Communications of the ACM 28 (1985), 1030 - 1044.
http://www.digicash.com/news/archive/bigbro.html

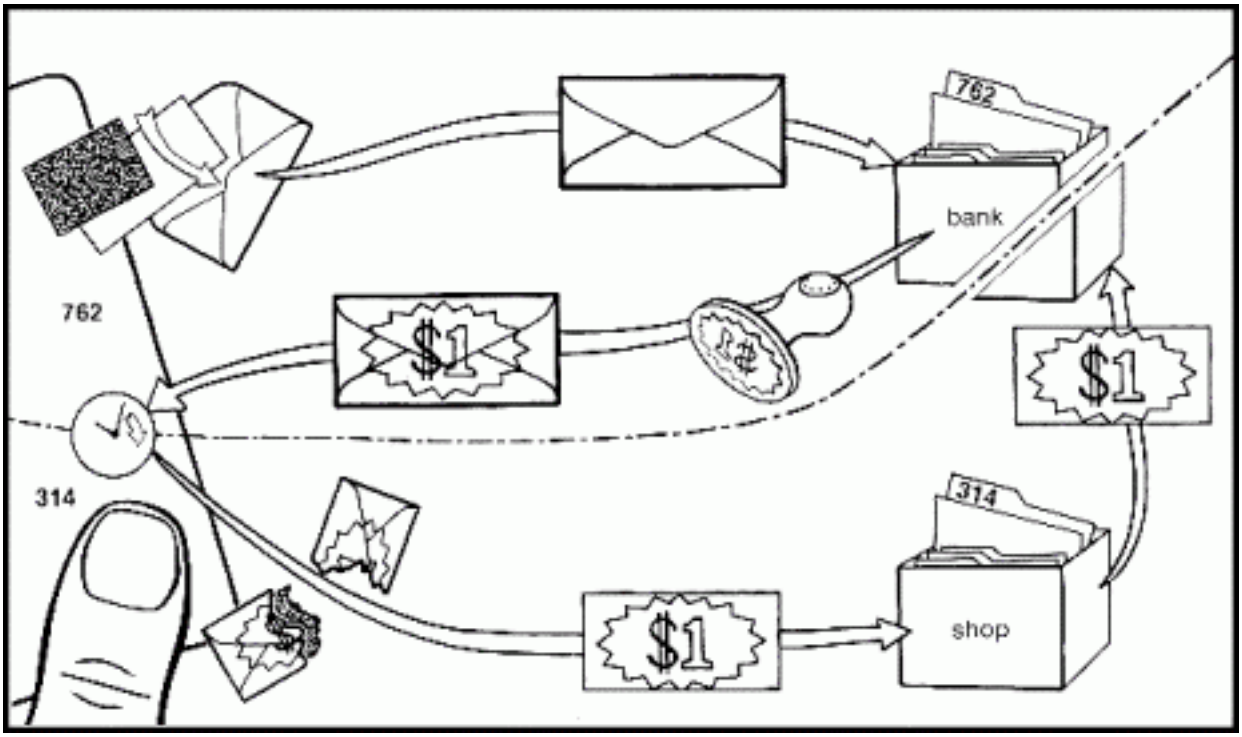
Klaus Pommerening: Chipkarten und Pseudonyme. FIfF Kommunikation 1/96, 9-12.
http://www.uni-mainz.de/~pommeren/Artikel/chipkarten.html

4. Elektronisches Geld

Echtes Hartgeld ist perfekt anonym, Papiergeld (durch die Seriennummer) verfolgbar (wichtige Ermittlungshilfe in Erpressungsfällen!).

Nicht-zuordenbares elektronisches Geld ist auch nichts anderes als eine Anwendungsform der Pseudonymisierung.

Das Protokoll in der Kohlepapier/Umschlag Metapher:



Ideale Eigenschaften elektronischen Geldes

- *Fälschungssicherheit*: Nur autorisierte Stellen können Geld anfertigen.
- *Universalität*: Das Geld kann über Netze übertragen und an beliebiger Stelle verwendet werden.
- *Offline-Verwendbarkeit*: An keiner Stelle des Protokolls ist eine Kommunikationsverbindung zu einer Bank oder anderen Zentralstelle nötig.
- *Einmalverwendbarkeit*: Das Geld kann nicht mehrfach ausgegeben werden.
- *Anonymität*: Niemand kann die Verbindung zwischen der Identität des Käufers und dem Kaufvorgang herstellen. (Außer Händler bei Sichtkontakt; Hauptanwendung ist aber anonymes Kaufen über ein Netz.)
- *Übertragbarkeit*: Das Geld kann an andere Besitzer weitergegeben werden.
- *Teilbarkeit*: Das Geld kann in Teilbeträgen ausgegeben werden.

Es gibt bisher kein realistisch durchführbares Protokoll, das alle diese Eigenschaften gleichzeitig verwirklicht.

Ein einfaches Protokoll könnte so aussehen:

Teilnehmer:

- A = Alice (Kundin)
- B = Bank
- H = Händler
- K = Klaus (Krimineller)

Herstellung einer elektronischen Münze (»Prägung«)

A möchte von der Bank B eine 100-S-Münze (gegen Abbuchung des Betrags von ihrem Konto).

Diese wird durch ein Pseudonym repräsentiert, das mit dem Wert 100 S verbunden und genau einmal verwendbar ist, und wie folgt erzeugt:

1. A generiert zufällige Seriennummer w.
2. A läßt w von B blind unterschreiben.

Verwendung einer elektronischen Münze

A will bei H mit ihrer 100-S-Münze bezahlen.

1. H prüft die Echtheit der Münze (mit öffentlichem Prüfschlüssel von B).
2. H reicht Münze bei der B ein.
3. B prüft die Echtheit und Erstmaligkeit.
4. B schreibt H 100 S gut.

Eigenschaften (nach diesem Protokoll)

1. A (oder K) kann kein Falschgeld erzeugen:

- Der Signaturschlüssel der Bank ist geheim.
- Erzeugen passender Seriennummer zu gegebener Unterschrift wird durch vorgegebene Struktur von w ausgeschlossen.

2. A bleibt vor H und B anonym (wie bei Pseudonymen); B kann die Münze nicht wiedererkennen.

3. B kann kein ungültiges Geld ausgeben; A prüft die Unterschrift nach Erhalt.

4. B ist vor Wiederverwendung sicher, wenn sie Seriennummer w bei Einlösung speichert.

5. B kann Wiederverwendung vortäuschen, um nicht zahlen zu müssen; dazu ist Kooperation mit (geeignetem) H notwendig.

6. H kann Münze als echt erkennen.

7. H ist vor Wiederverwendung nicht sicher, es sei denn, es existiert eine online-Verbindung oder Erweiterung des Protokolls.

8. K (auch H) kann Münze stehlen oder kopieren und selbst verwenden. A kann sich davor schützen, indem sie die Camouflage der blinden Unterschrift erst beim Bezahlen entfernt.

9. K kann A erpressen und Münze anonym verwenden. (Abhilfe: A verzichtet sofort auf ihre Anonymität und meldet w an B.)

Erweiterungen des Protokolls

- Berücksichtigung verschiedener Münzwerte
- Schutz von H vor Wiederverwendung
- Aufdeckungsmöglichkeit des Pseudonyms bei Betrugsversuch von A (durch Wiederverwendung)

Es gibt verschiedene Realisierungen im Web, einer der Pioniere - DigiCash - ist inzwischen eingegangen. Es gibt wenig interessante Kaufmöglichkeiten, und die Einsatzmöglichkeiten entwickeln sich viel langsamer als erwartet..

Politisch sind weniger anonyme Zahlungsmethoden bevorzugt (wg. Geldwäsche, Finanzmarktrisiken).

5. Elektronische Wahlen

Anforderungen an eine geheime Wahl

- *Wahlberechtigung:* Nur berechtigte Wähler können Stimmen abgeben.
- *Einmaligkeit:* Jeder Wähler kann nur einmal wählen.
- *Wahlgeheimnis:* Niemand kann feststellen, wie ein anderer gestimmt hat.
- *Fälschungssicherheit:* Niemand kann unbemerkt die Stimme eines anderen ändern.
- *Verifizierbarkeit:* Jeder Wähler kann sich überzeugen, daß seine Stimme korrekt gezählt wurde.

Zusätzlich bei manchen Typen von Wahlen:

- *Überprüfbarkeit:* Jeder kann feststellen, wer gewählt hat und wer nicht.
- *Überprüfungsschutz:* Ein Wähler kann gegenüber Dritten nicht nachweisen, wie er gewählt hat. (Soll Stimmenkauf mit anschließender Kontrolle verhindern.)

Wahlprotokoll mit Pseudonymen

1. Jeder Wähler erzeugt einen Satz von Nachrichten, eine für jede Wahlmöglichkeit.
2. Jede dieser Nachrichten wird zusammen mit einer zufälligen Seriennummer vom Wahlamt blind unterschrieben. (D.h. jeder registrierte Wähler hat dann für jede mögliche Stimme ein nur ihm bekanntes Pseudonym. Das Wahlamt kann durch Registrierung sichern, daß jeder Wähler nur einen Satz von Stimmen hat.)
3. Der Wähler verschlüsselt die seiner Wahl entsprechende Nachricht (Stimme, Seriennummer) zusammen mit der Beglaubigung mit dem öffentlichen Schlüssel des Wahlamts ...
4. Er sendet das Chiffrat ans Wahlamt.
5. Das Wahlamt entschlüsselt die Stimmen und zählt sie aus.
6. Das Wahlamt veröffentlicht das Wahlergebnis und dazu jede abgegebene Stimme zusammen mit der Seriennummer.

Damit sind die fünf Anforderungen erfüllt. Es ist aber noch organisatorische Kontrolle im Wahlamt nötig. Sonst

... könnten Wähler durch gefälschte Registrierung ausgeschlossen werden.
... könnte das Wahlamt beliebig viele zusätzliche Stimmen erzeugen.
... könnte das Wahlamt bei fehlender Senderanonymität die Stimmen den Wählern zuordnen.

Weiteres Problem: Ein Wähler kann mehrere verschiedene von seinen beglaubigten Stimmen abgeben (nur interessant, wenn mehr als zwei Wahlmöglichkeiten bestehen.)

Durch Erweiterung des Protokolls sind die Probleme weitgehend behebbar.

Pilotversuche

- Virtuelle Bundestagswahl [Telepolis, 23. 6. 1999]
- Wahlkreis 329 [Universität Osnabrück]
- Wahlen im Internet [Heise Newsticker, 23. 6. 1999]
- Wahlen im Internet [Telepolis, 23. 6. 1999]

6. Anonymität einer Nachricht

Anonymität ist eine weitergehende Forderung als Geheimhaltung einer Nachricht. Man will erreichen, daß

- der Absender einer Nachricht nicht rückverfolgbar ist (also anonym bleibt);
- durch Abhören des Netzes nicht zu erkennen ist, wer mit wem kommuniziert (»traffic analysis«).

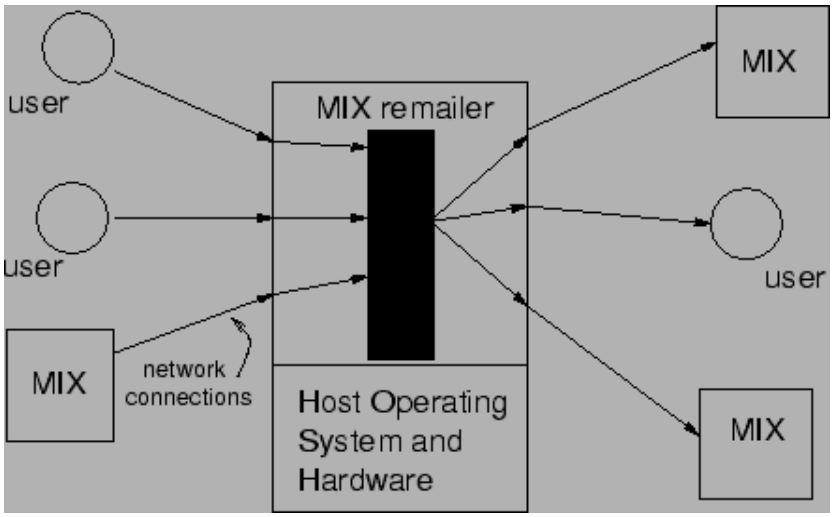
Zwei völlig unterschiedliche Realisierungen sind

- MIX-Netze (anonyme Remailer)
- (lokale) Ringnetze

Prinzip eines MIX:

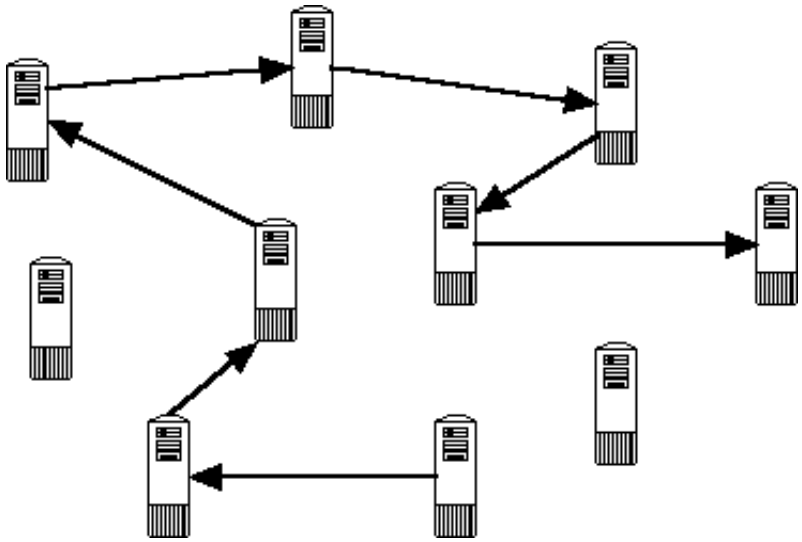
1. Jeder schreibt einen Brief (gleichzeitig).
2. Jeder steckt seinen Brief in einen kleinen Umschlag (Verschlüsselung mit öffentlichem Schlüssel des Empfängers) und adressiert ihn.
3. Jeder steckt den kleinen Umschlag in einen großen Umschlag (Verschlüsselung mit öffentlichem Schlüssel des MIX) und schickt ihn an den MIX.

4. Der MIX öffnet die großen Umschläge, wartet bis genügend zusammen gekommen sind (um Beobachtung des Ein-/Ausgangsverkehrs zu verhindern) und schickt jeden Brief an den eigentlichen Empfänger.



Das Prinzip wird im Internet (teilweise) bei »anonymen Remailern« realisiert.

Man kann die Sicherheit erhöhen, indem man die Nachricht durch eine Kette von MIXen verschickt.



Durch Erweiterung des Protokolls ist es auch möglich, daß der Empfänger einer anonymen Nachricht dem Absender antwortet, ohne ihn zu kennen.

Probleme mit MIXen

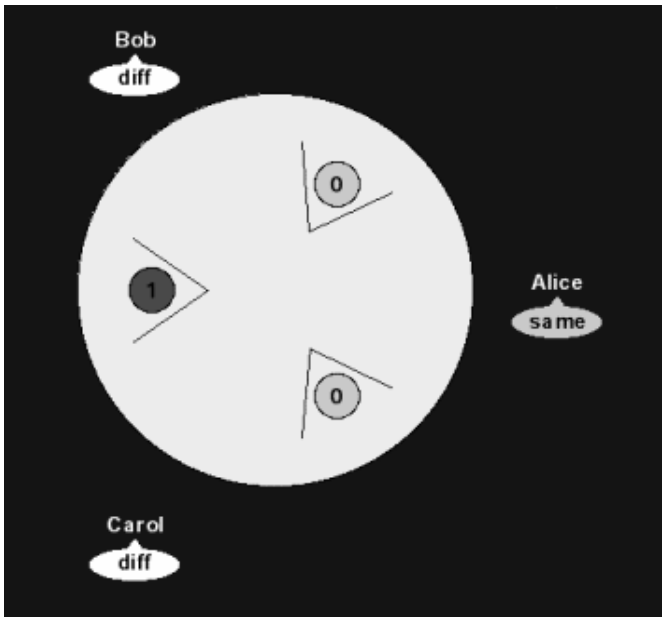
- MIXe müssen vertrauenswürdig sein. Lösung: Viele unabhängige MIXe.
- Trotzdem anfällig für mächtigen Netzüberwacher (staatlicher Geheimdienst).
- Netzlast vervielfacht
- MIXe sind Flaschenhälse.

Prinzip eines anonymen Ringnetzes:

Die Idee, wie in einem Ringnetz Nachrichten gesendet werden können, ohne daß jemand den Absender eruiren kann, läßt sich durch das »dining cryptographers problem« veranschaulichen:

> Drei Kryptographen essen in einem Restaurant, und als sie zahlen wollen, sagt der Kellner, daß die Rechnung schon beglichen wurde. Nun möchten sie herausbekommen, ob sie von einem der Anwesenden anonym eingeladen wurden oder ob NSA die Rechnung bezahlt hat.

Wie können sie das feststellen, ohne daß sich der mögliche Spender am Tisch zu erkennen ergibt?



Protokoll:

- Alle drei werfen hinter einer aufgestellten Speisekarte eine Münze.
- Jeder sieht von seinem Platz aus zwei Münzen und sagt, ob sie gleich oder ungleich sind.
- Wenn einer von ihnen gezahlt hat, muß er lügen.

Nun gilt: Wenn sich eine gerade Anzahl von »ungleich« ergibt, hat NSA gezahlt, bei ungerader Anzahl einer am Tisch.

Der Mechanismus kann mit einem Applet demonstriert werden, zu finden unter
http://www.nyx.net/~awestrop/crypt/dc-demo.htm

Gesellschaftspolitisch sind anonyme Kanäle nicht ganz unproblematisch, weil sie straflos Verleumdungen und Belästigungen ermöglichen (kann durch ein erweitertes Protokoll, das in bestimmten Fällen eine Aufhebung der Anonymität erlaubt, vermieden werden), und es zweifelhaft ist, ob eine Gesellschaft aus anonymen 'Personen' im öffentlichen Raum wünschenswert ist. In vielen konkreten Anwendungen erscheint ein solcher Mechanismus aber als sinnvoller Schutz gegen Überwachung und Verfolgung.

7. Secret Sharing

Für viele Anwendungen ist es sinnvoll ein Geheimnis (z.B. einen geheimen Schlüssel) so aufzuteilen, daß nur alle Besitzer zusammen das Geheimnis lüften können.
(Mehrschlüsselprinzip, verallgemeinertes Vieraugenprinzip)

Eine Verallgemeinerung kann durch (r, n)-Schwellwertschemata umgesetzt werden, bei denen r von n Teilgeheimnisinhabern erforderlich sind und weniger als r nichts ausrichten können. Z.B.

Ein Schloß kann genau dann geöffnet werden, wenn r beliebige Mitglieder einer Gruppe aus n Personen ihren Schlüssel anwenden.

Ein Dokument ist rechtgültig unterschrieben, wenn es von (mindesten) zwei der Unterschriftsberechtigten unterschrieben wurde.

Anwendungen:

- Schutz vor Einzeltätern,
- Schutz vor Schlüsselverlust
  (Geheimnis auf mehrere Orte verteilt, Entdeckung oder Zerstörung eines Teilgeheimnisses schadet nicht.)
- Geheime Nachricht auf mehrere Kanäle verteilen.
- Unterschriften bei Firmen

Schwellwertschema durch Polynom-Interpolation: (Shamir)

$q = a_0 + a_1X + \ldots + a_{r-1}X^{r-1}$, Polynom mit zufälligen ganzzahligen Koeffizienten,

wobei $S = q(0) = a_0$ der geheime Schlüssel (das verteilte Geheimnis) ist.

Als Teilschlüssel werden die Werte $S_i = q(x_i)$ für $x_i = i = 1, \ldots, n$ verteilt.

Die Berechnung von S erfolgt eindeutig mit Interpolationsformel bei r bekannten Wertepaaren (x_j, y_j); weniger als r Stützstellen lassen S völlig unbestimmt.

Eigenschaften solcher Schwellwertschemata:

- Die Zahl n der zugelassenen Personen ist jederzeit erweiterbar, ohne bisherige Teilschlüssel ändern zu müssen.
- Teilschlüssel sind änderbar (bei Verlust oder Entzug), ohne Gesamtschlüssel S zu ändern.
- Hierarchien sind modellierbar, indem bestimmte Personen mehrere Teilschlüssel erhalten.

8. Münzwurf per Telefon

Hierbei handelt es sich um ein Basis-Protokoll für geschäftliche Transaktionen bei gegenseitigem Mißtrauen, etwa um den Austausch von Ware und Geld zu gewährleisten, was in »real life« oft durch gleichzeitige Anwesenheit gewährleistet ist.

Jeder Partner kann bei einem Betrugsversuch des anderen die ganze Transaktion rückgängig machen.

Das Protokoll beruht auf einem »bit-commitment«, das man sich anschaulich so vorstellen kann:

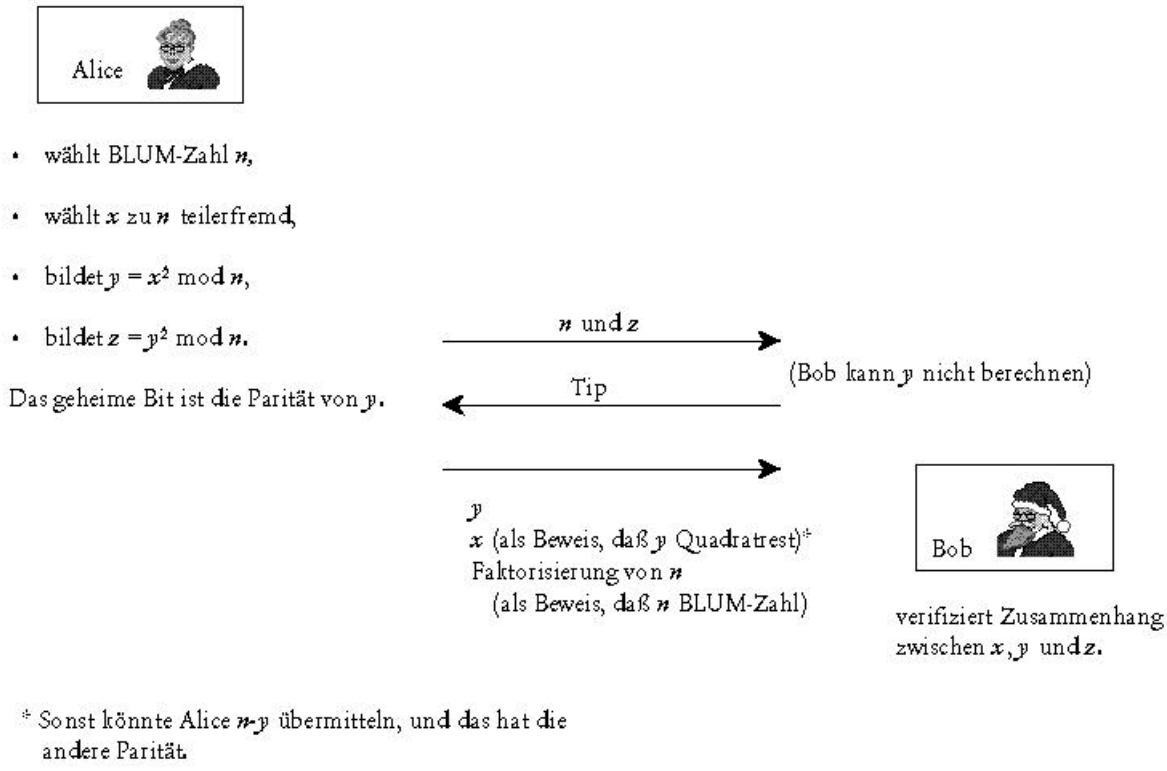
1. A packt ein Bit in eine Box, schließt sie zu, gibt sie B, behält aber den Schlüssel.
2. B gibt einen Tip ab, was drin ist.
3. A gibt B den Schlüssel, und
4. B öffnet die Kiste und schaut nach.

Beide wissen dann, ob B richtig getippt hat, keiner konnte schummeln.

Protokoll für einen Münzwurf per Telefon:

A (= Alice) teilt B (=Bob) den Wert eines Bits (»Münzwurf«) so mit, daß B ihn nicht ohne As Hilfe lesen kann.
B muß das Ergebnis raten.
A kann ihn nach der Mitteilung nicht mehr ändern kann.
Ob B richtig geraten hat, läßt sich für A und B feststellen.

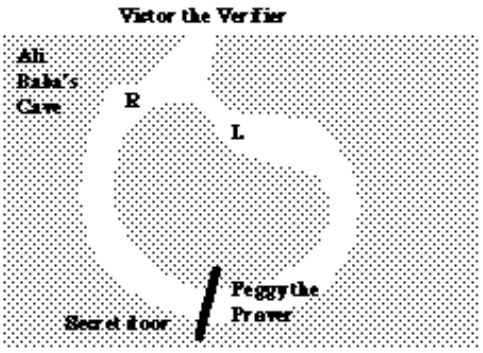
Ablauf des Protokolls



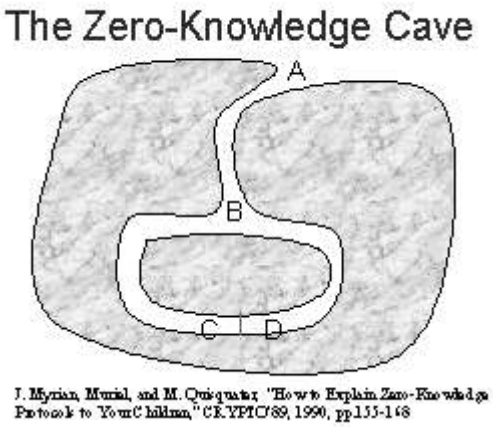
9. Zero- Knowledge-Protokolle **(Beweise ohne Wissenspreisgabe)**

Peggy (»Prover«) hat ein Geheimnis und kann Victor (»Verifier«) davon überzeugen, daß sie es hat, ohne das Geheimnis preiszugeben (auch nicht teilweise).

Das Prinzip eines Zero-Knowledge Beweises kann mit einem 'Höhlengleichnis' veranschaulicht werden:



oder



Peggy behauptet die geheime Tür zwischen C und D öffnen zu können und will Victor davon überzeugen, ohne ihm etwas darüber zu verraten.

Protokoll:

- Sie begibt sich nach unten in die Höhle in einen beliebigen Gang.
- Victor geht in die Höhle zum Punkt B.
- Er wählt zufällig 'links' oder 'rechts' und ruft, Peggy möchte im entsprechenden Gang erscheinen.

Falls Peggy die Tür nicht öffnen kann, kann sie nur mit 50%iger Wahrscheinlichkeit richtig reagieren.

Die beiden wiederholen das Spiel n-mal, und Victor überzeugt sich (mit einer Irrtumswahrscheinlichkeit von $1/2^n$) davon, daß Peggy das Geheimnis der Tür kennt, ohne sonst etwas darüber zu erfahren.

Hauptanwendung: Identifikation und Zugangskontrolle (implementiert mit Chipkarten)

Anforderungen:

- Vollständigkeit: Jeder echte »Ausweis« wird als echt erkannt.
- Korrektheit: Jeder falsche »Ausweis« wird als falsch erkannt.
- Keine Wissenspreisgabe: Der Kontrolleur erwirbt keinerlei Wissen über das Geheimnis. (Insbesondere kann er den Ausweis nicht kopieren oder nachmachen.)
  [Diese Anforderung läßt sich beweisfähig formalisieren.]

Vorteil: Kein online-Zugriff auf Schlüsselverzeichnis nötig.

Ablauf:

a) Initialisierungsphase

Vertrauenswürdige Zentrale C vergibt an Teilnehmerin B:

- Identitätsbezeichner (öffentlich sichtbar),
- zugehöriges Geheimnis.

C speichert keine Daten und hat nichts mit der Anwendungsphase zu tun.

b) Anwendungsphase

Ein Prüfer V prüft die Teilnehmerin P;

er stellt fest, ob A das zu ihrem Identitätsbezeichner gehörige Geheimnis kennt,
ohne das geringste über es zu erfahren.

Beispiel: das Fiat/Shamir-Identifikationsschema *(npr)*

a) Initialisierung

Die Zentrale C besitzt

- eine Blum-Zahl n, die öffentlich bekannt ist,
- die Primzerlegung $n = p*q$ als großes Zentralgeheimnis.

Die Zentrale erzeugt für die Teilnehmerin A

- eine Identifikationsnummer I_A (große ganze Zahl, Quadratrest),
- als zugehöriges Geheimnis die Quadratwurzel s (mod n) aus I_A^{-1}.

(Bemerkung: Damit I_A mit hinreichender Sicherheit ein Quadratrest ist, enthält es ein Dummy-Feld, das geeignet besetzt wird.)

b) Anwendung

- A wählt Zufallszahl r, bildet $x = r^2 \bmod n$, sendet x an B.
- B wählt zufälliges Bit b, sendet b an A.
- Falls b = 0, wählt A die Zahl y = r;
  falls b = 1, wählt A die Zahl $y = r * s \bmod n$.
- A sendet y an B.
- Falls b = 0, prüft B, ob $x = y^2 \bmod n$ und überzeugt sich, daß A die Wurzel aus x kennt;;
  falls b = 1, prüft B, ob $x = y^2 * I_A \bmod n$ und überzeugt sich, daß A die Wurzel aus x/I_A kennt.

c) Eigenschaften

Vollständigkeit: Falls A das Geheimnis s kennt, kann sie immer korrekt antworten.

Korrektheit: Falls A in Wirklichkeit Ã ist, also das Geheimnis s nicht kennt, kann sie höchstens eine der beiden Fragen richtig beantworten.
(Sonst könnte sie die Quadratwurzel aus $1/I_A$ ziehen)

Ã kann also die zufällige Frage (abhängig von b) nur mit Wahrscheinlichkeit höchstens gleich 1/2 richtig beantworten. Nach t Runden des Protokolls hat Ã also nur eine Erfolgswahrscheinlichkeit von höchstens $1/2^t$.

Kryptographische Infrastruktur

1. Schlüsselmanagement

PKI (Public Key Infrastructure) - Management von öffentlichen Schlüsseln

Komponenten einer PKI (Public Key Infrastructure)

- Öffentliche und private Schlüssel.
- Schlüsselerzeugung und Schlüsselaufbewahrung.
- Zertifikate und Trustcenter.
- Verzeichnisdienste.
- Standards, Schnittstellen, Portabilität.
- Integration in Anwendungen, Systemdienste und Benutzungsoberflächen.
- Kryptographische Bibliotheken.

Umgang mit Schlüsseln

Durch die kryptographischen Techniken, insbesondere durch die Verwendung von asymmetrischer Kryptographie und von Chipkarten, wird eine organisatorische Komplexität bedingt, die aber weitgehend in den Verwaltungs- und Anwendungsprogrammen versteckt werden kann, z. B. in die Benutzerverwaltung. Vor dem Benutzer selbst kann die Komplexität soweit versteckt werden, daß er kaum einen Unterschied zur »klassischen« Paßwort-Handhabung merkt. Folgende Fragen sind zu behandeln:

Wie werden Schlüssel erzeugt?
Wer erzeugt Schlüssel?
Wie werden Schlüssel verteilt?
Wie werden Schlüssel sicher aufbewahrt?
Wie werden Schlüssel sicher verwendet?
Wer darf welche Schlüssel kennen?
Wie lange sind Schlüssel gültig?
Wie werden Schlüssel gewechselt?

Schlüsselerzeugung und -aufbewahrung von geheimen Schlüsseln sollte niemand anderem anvertraut werden.

Management privater Schlüssel - Schlüsselaufbewahrung, Aufteilung von Schlüsseln

Komponenten der privaten Schlüsselverwaltung

- Schlüsselerzeugung:
  - sicheres Programm ohne Trojanische Pferde,
  - gute Zufallsquelle,
  - sichere Umgebung.
- Schlüsselaufbewahrung:
  - sicheres Medium (Chipkarte),
  - PIN oder Paßphrase,
  - Backup,
  - Keyserver för öffentliche Schlüssel.
- Schlüsselverteilung (öffentliche Schlüssel):
  - Extraktion in portabler Form,
  - Zertifikate (eigen oder durch Institution),
  - Keyserver oder öffentliches Verzeichnis,
  - »Fingerabdruck« zur Verifikation (Hash).

Wieviele Schlüssel braucht der Mensch?

Mindestens je ein Schlüsselpaar für die Anwendungen

- asymmetrische bzw. hybride Verschlüsselung,
- digitale Signatur,
- starke Authentisierung,

sonst gibt es Probleme - wie das versehentliche Entschlüsseln anstelle einer vermeintlichen Signatur (»RSA-Falle«).

Ferner weitere Schlüsselpaare für

- Pseudonyme,
- blinde Unterschrift,
- und weitere Spezialanwendungen.

Das PSE (= Personal Secure Environment, »persönlicher Schlüsselkasten«)

Inhalt des PSE = Alle nötigen Sicherheitsinformationen:

- Schlüssel für Anwendungen,
- private Schlüssel (Verschlüsselung, Signatur, Authentisierung),
- zugehörige Zertifikate,
- öffentliche Schlüssel von Zertifikatsstellen,
- weitere vertrauenswürdige öffentliche Schlüssel.

PSE wird mit PIN (Geheimzahl, Paßwort) abgesichert. Der Besitzer merkt sich nur die PIN (und verwahrt das PSE sicher).

Gute Realisierung mit Chipkarte.

Bei PGP: Geheimer Schlüsselring (secring) als Datei, die mit Passphrase (»Mantra«) verschlüsselt ist.

2. Kryptographische Software (Beispiele)

Sicherheitsprobleme bei E-Mail

- Abhören (z. B. durch Netzbetreiber, Systemverwalter).
- Fehlzustellung.
- Ablage in der privaten Mailbox (im File-System).
- Manipulation des Absenders.
- Fälschung des Inhalts.
- Fälschung des Sendenachweises.
- Nicht vorhandener oder gefälschter Empfangsnachweis.
- Zustellung nicht garantiert.

Bsp.: **Pretty Good Privacy**

Philip Zimmermann, MIT, seit 1990, inzwischen kommerziell (Network Associates)
Internet-Standard OpenPGP in Entwicklung,
GNU-PGP als Open-Source Variante

Kryptographie für alle:

- Verschlüsselung mit hybridem Verfahren (RSA + IDEA, DH + IDEA/CAST/3DES).
- Digitale Signatur (MD5 + RSA, DSS).
- Schlüsselverwaltung.

- auf alle wichtigen Systeme (kompatibel) portiert (MS-DOS, MS-Windows, UNIXe, VMS, Mac..)
- in die wichtigsten E-Mail-Programme integrierbar.

Weitere Bestandteile

- Schlüsselringe: persönliche Verzeichnisse von asymmetrischen Schlüsseln
- geheime Schlüssel ($PGPPATH/secring.pgp)
- öffentliche Schlüssel von Kommunikationspartnern ($PGPPATH/pubring.pgp)
- Paßphrase (Mantra): An der Geheimhaltung hängt die ganze Sicherheit. (Auf Mehrbenutzersystemen nicht absolut sicher zu halten.)
- Fingerabdruck (finger print) zur telefonischen Verifikation
- Zertifizierung fremder Schlüssel.
  Statt einer allgemein anerkannten Zertifikatsinstanz werden öffentliche Schlüssel neuer Partner durch gemeinsame vertrauenswürdige Bekannte zertifiziert (»web of trust«).
- Zufallsgenerator (»physikalisch«: Zeitabstände von Tastendrücken) Erzeugung von symmetrischen Einmalschlüsseln, Erzeugung von asymmetrischen Schlüsseln.

Anwendungen

- E-Mail verschlüsseln und signieren.
- Dateien von Hand verschlüsseln (z. B. zum Filetransfer).

Schwachstellen

- Vertrauen in Arbeitsumgebung nötig (für Mehrbenutzersysteme nicht empfohlen, kein Schutz vor Trojanischen Pferden.)
- Echtheit von Schlüsseln? Keine vertrauenswürdige Zentrale.
- Kommerzielle Weiterentwicklung umstritten.

Nicht direkt einsetzbar für

- Filesystem-Verschlüsselung.
- Integration in Anwendungen (z. B. Datenbank).
- Integration in Systemdienste.
- Chipkarten als Sicherheitsausweis.
- Andere kryptographische Protokolle.

Für und wider:

+ Verfügbare, funktionierende, handhabbare kryptographische Software.
+ Verfügbarkeit auf (fast) allen Plattformen (kompatibel!).
+ Einsatz sehr sicherer Algorithmen.
+ kostenlos.
+ Weit verbreiteter Quasi-Standard.

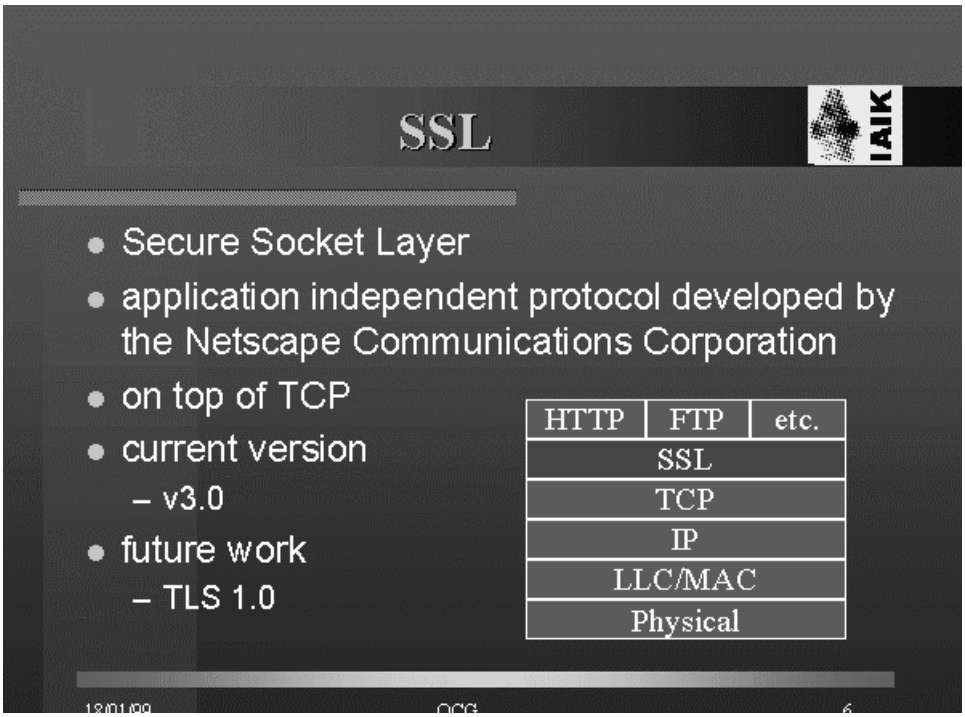
- Schlüsselspeicherung nicht sicher vor Trojanischen Pferden (z. B. PGPcrak).
- Zertifikats-Infrastruktur nicht organisiert.
- Versionen-Wirrwarr, nicht abwärtskompatibel.

Internet-Ressourcen

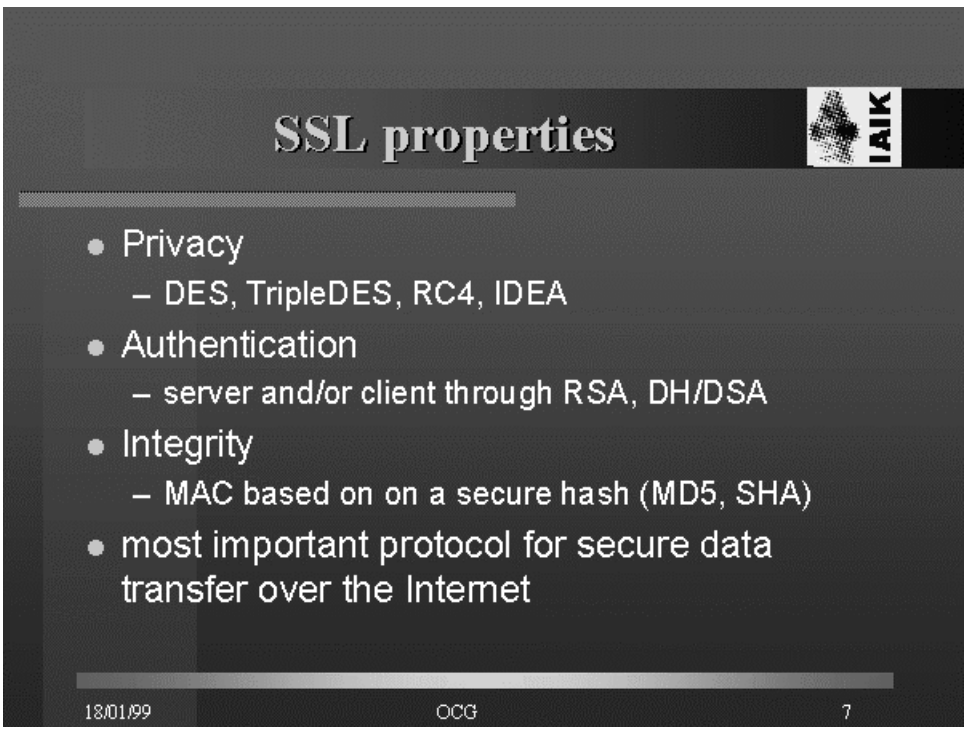
Pretty Good Privacy Home Page [http://www.pgp.com]
The International PGP Home Page [http://www.pgpi.com/]
Nichttechnische Einführung zu PGP [http://www.iks-jena.de/mitarb/lutz/anon/pgp.html]
Deutsche Anleitung zu PGP [http://home.kamp.net/home/kai.raven/pgp5kurs.htm]
PGP-FAQ von c't [http://www.heise.de/ct/pgpCA/faq.shtml]

SSL-Handshake Protokoll

Die **Secure Sockets Layer (SSL)** Protokollschicht liegt unterhalb der Anwendungen auf dem TCP/IP Protokoll auf.

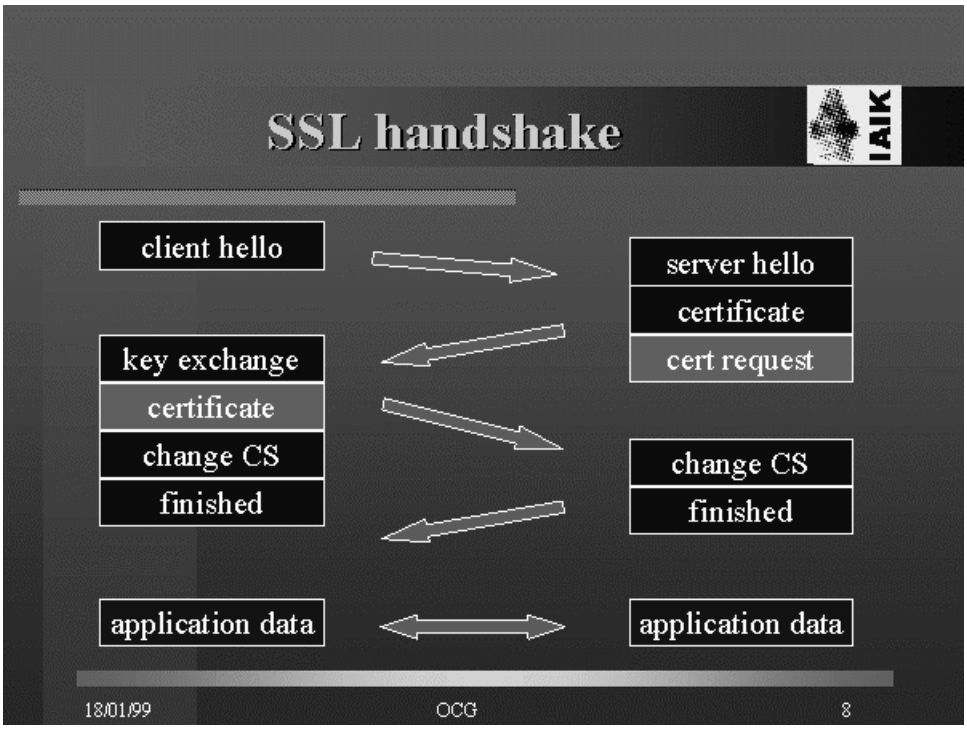


SSL enthält eine Reihe von kryptographischen Verfahren (asymmetrische und symmetrische Verschlüsselungen, Schlüsselaustauschverfahren, Signatur-Schemata, MACs und Hash-Funktionen) mit unterschiedlichem Sicherheitsniveau.



Das **Handshake-Protokoll**, bei dem der Server (Klient) durch ein Zertifikat einer »Certificate Authority« authentifiziert wird, funktioniert (vereinfacht) wie folgt:

- Client sendet eine »Hello«-Nachricht an Server, die seine SSL-Versionsnummer und andere Daten enthält.
- Server antwortet mit ähnlichem Hello und sendet außerdem ein Zertifikat, daß er der richtige Server ist. (U.U verlangt er vom Client ebenfalls ein Zertifikat über dessen Identität.)
- Client authentifiziert mit dem Zertifikat die Identität des Servers.
- Beide einigen sich über eine symmetrische Verschlüsselung und ein asymmetrisches Schlüsselaustauschverfahren (meist »RSA key-exchange«).
- Client sendet Server ein »premaster secret«, das er mit dessen authentifiziertem öffentlichen Schlüssel verschlüsselt, woraus beide (nachdem der Server es mit seinem geheimen Schlüssel 'ausgepackt' hat) das »master secret« berechnen.
- Beide gewinnen aus dem »master secret« den Session-Key, der für die gewählte symmetrische Verschlüsselung verwendet wird.
- Nun beginnt die SSL-Session mit dem eigentlichen Datenverkehr zwischen Client und Server.



Eine genauere Beschreibung findet man unter
http://developer.netscape.com/docs/manual/security/sslin/contents.htm

3. Hardware-Unterstützung der kryptographischen Infrastruktur

Chipkarten (smart cards)

Chipkarten sind Computer im Scheckkartenformat.

Die persönliche »Ausweiskarte«:

- enthält die Zugriffsberechtigungen (in Form der nötigen kryptographischen Schlüssel),
- führt die digitale Signatur aus,
- ist PIN-gesichert (Sicherung durch Besitz und Wissen),
  (In Entwicklung: biometrische Merkmale)
- könnte auch Pseudonyme enthalten.

Technik

- Single Chip Computer,
- 8-bit-CPU, bis 2 MIPS,
- Arbeits-, Programm- und Datenspeicher (z. B. 256 Bytes RAM, 10 KB ROM, 8 KB EEPROM),
- Chipkarten-Betriebssystem,
- Ein- und Ausgabekanal.

Normierung

- Maße (85.6 mm x 54 mm x 0.76 mm),
- Widerstandsfähigkeit (Biegung, Verdrehung, Hitze, Strahlung, elektromagnetische Felder, Chemikalien, ...) (=> Chipfläche auf ca. 25 mm^2 beschränkt),
- Anordnung der Kontakte,
- Kommunikationsprotokolle,
- Datenstrukturen und Sicherheitsattribute (im Diskussionsstadium).

Chipkarten sind (angeblich) gesichert vor

- Ausspähung gespeicherter Geheimnisse (z. B. kryptographischer Schlüssel),
- Manipulation (z. B. gespeicherter Geldbeträge).

Technische Sicherheitsvorkehrungen:

- Nicht direkt lesbare Speicher,
- Zugriff nur über I/O-Port, CPU und Sicherheitsmodul,
- manipulationssichere Verschweißung mit Selbstzerstörungsmechanismen.

Sicherheitseigenschaften (mögliche)

- PIN-Schutz, Überprüfung durch interne Logik.
- Selbstsperrung nach (meist 3) Fehlversuchen.
- Interne Verschlüsselungsfunktionen.
- (Evtl.) verschlüsselte Speicherung der Nutzdaten.
- Chiffrierter Datenaustausch (langsam!).

Anwendungen

- Telefonkarten,
- Krankenkassenkarte (Ersatz für Krankenschein),
- Geldkarte,
- Sicherheitssysteme (Identifikation, PSE/PCT),
- Health Professional Card (HPC).

Für und wider:

+ Sicherheit für jedermann auf höchstem Niveau,
+ Speicherung geheimer Informationen (z. B. Schlüssel)
+ Ausführung von kryptographischen Algorithmen,
+ einfache Benutzung.

- Standardisierung noch nicht abgeschlossen.
- Kosten der Karte (10 - 30 DM, je nach Funktionalität).
- Infrastruktur (Lese- und Schreibgeräte, Verwaltung).

Chipkarten sind längst nicht so sicher, wie allgemein angenommen.

Dazu später etwas mehr.

Biometrische Authentisierung (eigentlich: anthropometrische Authentisierung)

Ziel: Ablösung der PIN oder des Paßworts, um die bekannten Probleme zu vermeiden.

Schlagzeilen (Computer-Zeitung Ende 1998)

- »Der Körper selbst wird zum Ausweis.« (Schneier: »You are your key.«)
- »Fingerabdrucksysteme sind zur Zeit am weitesten gereift.«
- »Fingerabdruck weckt ungute Assoziationen.«
- »Branche gibt Kombination aus Fingerprint-Check und Chipkarte die besten Chancen.«
- »Noch zwei Jahre bis zum Durchbruch.«

Geeignete biometrische Techniken

Merkmal:	***Hardware***:	***spezielle Probleme***:
Struktur der Iris	Kamera	Kontaktlinsen
Gesicht	Kamera	
Mimik(z. B. Lippenbewegung)	Kamera	
Stimme	Mikrofon	Heiserkeit
Fingerabdruck	Sensor	Verschmutzung, Verletzung
Handgeometrie	Scanner	Platzbedarf
Unterschriftsdynamik	Spezielle Unterlage	Platzbedarf
Tipprhythmus	Tastatur	Länge des Texts (1 Zeile)
DNA	(Spucknapf?)	Datenschutz

Allgemeine Probleme I

- Akzeptanz? (Erkennungsdienstliche Behandlung vs. Nachvollziehbarkeit)
- Datenschutz? (Universelle Datenspuren, elektronische Überwachung? Politischer Mißbrauch?)
- Infrastruktur? (Zentrale Datenbanken? Normen?)
- Kosten?
- Komplexität der zugehörigen Software?
- Fälschungssicherheit? (Auch zwischen Digitalisierung und Abgleich?)
- Störanfälligkeit?
- Adjustierung der Sicherheitsschwelle (Sensitivität/Spezifität)?
- Normierung?

Allgemeine Probleme II (Schneier)

- »Biometrische Merkmale sind eindeutige Identifikatoren, aber keine Geheimnisse.«
- Keine »Schlüsseländerung« möglich.
- Charakteristiken eines Schlüssels: Geheimhaltung, Zufälligkeit, Änderbarkeit, Zerstörbarkeit.
- Bei »Verlust« geht nichts mehr. (Finger ab => Auto springt nicht an.)

Biometrische Merkmale sind geeignet in Situationen, wo der Weg vom Sensor zum Verifikator vertrauenswürdig ist (z.B. lokale Authentisierung gegenüber Chipkarte).

Sicherheit?

Der Chaos-Computer-Club (CCC) hat berichtet, wie sie die gängigen biometrischen Verfahren überlistet haben.

4. Zusammenfassung

Wie weit ist die Infrastruktur in der Praxis vorhanden?

- Kryptographische Basistechniken

  ... sind voll entwickelt, Programm-Moduln sind verfügbar (z. B. RSA, 3DES, ...).

- Kryptographische Protokolle

  ... sind voll spezifiziert, Programm-Moduln sind weitgehend verfügbar (z. B. PGP, SSL, Kerberos, ...).

- Sicherheitssysteme

  ... sind z. T. verfügbar, ihre Integration in den laufenden Betrieb ist oft noch schwierig (z. B. Firewall-Systeme, Chipkarten, kryptographische Filesysteme).

- Sichere Informationssysteme

  ... sind kaum vorhanden!

IT-Sicherheit in offenen und verteilten Systemen verlangt zwingend kryptographische Mechanismen.

Hindernisse für den Einsatz von Kryptographie

- US-Exportbestimmungen und sonstige Kryptographie-Regulierungen (negative Auswirkungen auf Weltmarkt und internationale Normen)
- Ignoranz auf Seiten der Hersteller (kein kryptographisches Know-How)
- negativer PR-Effekt von »Angstmache«
- Mißverständnisse über Komplexität, Performanz und Kosten kryptographischer Verfahren.
- Fehlende Marktstabilität (z. B. verbreitete Standards)
- Fehlende Infrastruktur (Zertifizierungsdienste als Anfang)
- keine hinreichend einfachen Benutzungsschnittstellen.
- »Hauptsache das System läuft.« Einstellung

Die Hersteller

- sind anzuhalten, die nötigen Sicherheitsfunktionen in ihre Systeme zu integrieren.
- sollten Schutz-ignorante Technik vermeiden.
  (Datenmüll, schwache Verschlüsselung, reiner Paßwortschutz, ...)
- sollten das nötige sicherheitstechnische Know-How erwerben.

Kennzeichen für fehlendes Know-How:

> »Unser Produkt ist sicher.« - ohne genaue Dokumentation.
> »Der Zugriff ist sicher, weil paßwortgeschützt.«
> »Wir verwenden ein selbstentwickeltes Verschlüsselungsverfahren.«

Die technische Entwicklung ist schon seit Jahren so weit, die Produkte sind aber noch nicht auf dem Markt etabliert und werden auch nicht als notwendig empfunden.

Es wäre Aufgabe des Gesetzgebers, weitergehende Sicherheitsauflagen für Herstellung und Gebrauch von IT-Systemen vorzuschreiben (analog Sicherheitsgurten im Auto).

Auch im Privacy-Bereich reicht der gesetzliche Zwang der Datenschutzgesetze nicht, da er die Last den Systembetreibern aufbürdet, die die Daten verwalten, und nicht den Systemherstellern.

Grenzen der Kryptographie

Es stellt sich die Frage, welche der Dimensionen der Verläßlichkeit durch kryptographische Verfahren und Protokolle (im Prinzip) zufriedenstellend gewährleistet werden können.

Es gibt starke kryptographische Maßnahmen für

- Echtheit,
- Verbindlichkeit,
- Vertraulichkeit,

aber diese hängen auch von den Umgebungsbedingungen ihres Einsatzes ab.

Nur schwache Schutzmaßnahmen gibt es für

- Verfügbarkeit und
- Einmaligkeit.

Wogegen Kryptographie *nicht* schützt:

- Protokoll-Attacken,
- Trojanische Pferde,
- Viren,
- Denial-of-Service Attacken
- elektromagnetische Abstrahlung, Lauschangriff,
- physische Unsicherheit,
- Fehler im Betriebssystem,
- Fehler in Anwendungsprogrammen,
- Hardwarefehler,
- Anwenderfehler,
- Leichtsinn
- Social Engineering,
- »Dumpster Diving« (Abfallverwertung).

Nicht-kryptographische (technische und organisatorische) Sicherheitsmaßnahmen:

- Physische Sicherheit von Rechnerräumen, Archiven und Netzen (bauliche Sicherheit, Zutrittssperren)
- Vernichtung von Informationsträgern
- Wartung (und Vorführung) mit Testdaten
- Schulung von Benutzern und IT-Personal
- Klare Zuständigkeitsregeln und Verpflichtungen
- Überwachung und Protokollierung
- Paßwort-Regeln (vorläufig, entfällt mit Chipkarten-Lösungen oder biometrischer Authentisierung)
- Zugriffsregelungen und deren Verwaltung in verteilten Systemen
- Schwachstellen- und Gefährdungsanalysen
- Entwicklung von Sicherheitsmodellen und Sicherheitskonzepten
- Dokumentationen (Sicherheitskonzept, Maßnahmen, Zuständigkeiten)
- Sicherheitskontrollen, Zugriffskontrollen