Proc. Verläßliche Informationssysteme (VIS'95), Vieweg, 1995

Vertrauenswürdiger Entwurf portabler Benutzerendgeräte und Sicherheitsmodule

Andreas Pfitzmann

Technische Universität Dresden
Institut für Theoretische Informatik
01062 Dresden
pfitza@tcs.inf.tu-dresden.de

Birgit Pfitzmann,
Matthias Schunter

Universität Hildesheim
Institut für Informatik
Marienburger Platz 22
31141 Hildesheim
{pfitzb,schunter}@informatik.
uni-hildesheim.de

Michael Waidner[1]

IBM Forschungslaboratorium Zürich
Säumerstrasse 4
CH-8803 Rüschlikon, Schweiz
wmi@zurich.ibm.com

Zusammenfassung: Portable Benutzerendgeräte (POBs) und Sicherheitsmodule (SMs) müssen hohe Sicherheitsanforderungen erfüllen, um für Anwendungen wie elektronische Zahlungssysteme oder elektronisches Unterschreiben von Dokumenten einsetzbar zu sein. Insbesondere müssen die Benutzer selbst ihren POBs und SMs vertrauen können. Es werden daher praktikable „vertrauensbildende" Maßnahmen für Entwurf, Entwicklung, Produktion, Initialisierung und Nutzung von POBs und SMs vorgestellt. Insbesondere werden Methoden zur Unterschrift großer Dokumente auf kleinen POBs und Alternativen zu Smartcards für SMs vorgestellt sowie flexiblere Verfahren zur Benutzeridentifikation diskutiert.

1 Einleitung

Was sind *portable Benutzerendgeräte* (POB) und *Sicherheitsmodule* (SM)?

POBs sind beliebige tragbare Geräte mit Rechen- und Speicherleistung, wie zum Beispiel tragbare Rechner (Notebooks, PDAs), Mobilfunktelefone, Taschenrechner, Digitaluhren, Gameboys, sogenannte elektronische Brieftaschen oder einfach Prozessorchipkarten (*smart cards*).

SMs sind manipulationssichere (*tamper-resistant*) Rechner, die versuchen, die

---

[1] Die Arbeiten wurden größtenteils am Institut für Rechnerentwurf und Fehlertoleranz, Universität Karlsruhe, ausgeführt.

Vertraulichkeit und Integrität gespeicherter Daten auch bei physischen Angriffen zu wahren. Einfache SMs sind Prozessorchipkarten [GuUQ 92]; leistungsfähigere und komplexere Module sind jedoch bereits erhältlich [Palm 92].

Ein Benutzerendgerät kann zugleich ein Sicherheitsmodul sein oder ein oder mehrere SMs enthalten.

Betrachtet werden unter anderem folgende Anwendungen:

- Elektronische Off-Line Zahlungssysteme (*electronic cash*) mit elektronischen Brieftaschen und Chipkarten als SMs. Solche Systeme werden zur Zeit z.B. von National Westminster (*Mondex*) [Rolf 94] und vom europäischen ESPRIT-Forschungsprojekt „CAFE“ entwickelt [BBCM 94][2], wobei sich das CAFE-System durch die fortschrittlichste Architektur und Kryptographie auszeichnet.
- Mobilfunktelefone [ETSI 90] und Vorschläge zur Erhebung von Straßennutzungsgebühren analog den Zahlungssystemanwendungen [MeMä 94].
- Elektronisches Unterschreiben von Dokumenten für das „papierlose Büro“ und elektronische Abwicklung von Rechtsgeschäften. Bisherige Erfahrungen mit derartigen Anwendungen auf Personalcomputern zeigen, daß rechtsgültige Unterschriften ohne benutzereigene Geräte nicht machbar sind: Einfache Gerätemanipulationen sind vom Benutzer nicht erkennbar und ermöglichen das Erlangen von Unterschriften, die der Unterzeichner nicht beabsichtigte [Pord 93, PoRS 93].

Um praktische Sicherheit zu erreichen, müssen die Anwendungen insgesamt betrachtet werden: Sicherheit scheitert oft an der Faulheit der Benutzer. Der Benutzer will weder viele POBs oder SMs verwalten noch sein Geld auf mehrere Geräte verteilen müssen. Außerdem sollte ein POB auch für weniger sicherheitsrelevante Anwendungen ohne große Umstellungen brauchbar sein. Es wird im folgenden vorausgesetzt:

- Jedes Gerät (POB/SM) ist einem Benutzer fest zugeordnet (im Gegensatz etwa zu öffentlichen Terminals).[3]
- Die Anwendung schließt ein Rechtsgeschäft ein, d.h. der Benutzer gibt mittels seines POBs eine Willenserklärung ab. Der Benutzer muß daher den Ablauf prüfen und wichtige Schritte autorisieren können, z.B. bei einer Zahlung sowohl den Betrag als auch die Weitergabe persönlicher Daten.

In Kap. 2 geben wir einen Überblick über verschiedene Arten von Vertrauen in

---

[2] Unsere Forschungsgruppe ist an CAFE beteiligt. Unsere Erfahrungen aus diesem Projekt motivierten uns, dieses Papier zu schreiben.

[3] Sollen Geräte verliehen oder von Gruppen geteilt werden, ist zumindest ein minimales sicheres Mehrbenutzerbetriebssystem nötig. Dies wird im folgenden nicht betrachtet.

POB und SMs und über „vertrauensbildende“ Entwicklungs- und Herstellungsmethoden. Anschließend werden einige Fragestellungen genauer betrachtet, die bisher in der Literatur nicht oder nicht umfassend behandelt wurden:

- Wie kann das Vertrauen von Benutzern, deren Sicherheit von einem POB/SM abhängt, in ihre Geräte erhöht werden (Kap. 3)?
- Wie können die Handlungen des Gerätes für Benutzer nachvollziehbar gemacht werden (Kap. 4), insbesondere bei beschränkten Ein- und Ausgabemöglichkeiten?
- Maßnahmen gegen Verlust der Geräte (Kap. 5).
- Flexible Maßnahmen zur gegenseitigen Erkennung von Benutzer und Gerät (Kap. 6).
- Mehr über sicheren Speicher in Sicherheitsmodulen (Kap. 7).

Diese Gliederung folgt dem Lebenszyklus eines Geräts mit Untergliederung nach den verschiedenen Vertrauensarten.

2 Vertrauen ist nicht gleich Vertrauen

2.1 Drei Arten von Vertrauen

Wir unterscheiden folgende Arten von Vertrauen nach Situation des Agenten (d.h. des SM/POB, das für eine Person handelt):

1. *Vertrauen in persönlichen Agenten:* In den hier betrachteten Anwendungen müssen die Benutzer darauf vertrauen, daß ihre Geräte, während sie diese besitzen, korrekt arbeiten, z.B. kein Geld löschen und keine beliebigen Nachrichten unterschreiben.
2. *Agent unter fremder Kontrolle*: Meist müssen POBs und SMs auch bei Angriffen in der Lage sein, Schaden zu verhindern. Wir unterscheiden zwei Arten von fremder Kontrolle über ein Gerät:

   2a. *Vertrauen in entführten Agenten*: Hier vertraut der rechtmäßige Benutzer darauf, daß auch ein verlorenes oder gestohlenes Gerät seine Rechte sichert. Ähnliche Situationen sind Wartung und vorübergehende Weitergabe, z.B. in ein POS-(Point-of-Sales-)Terminal.

   2b. *Vertrauen in Agenten in feindlicher Umgebung*: Jemand gibt sein Gerät dauerhaft an Dritte weiter und vertraut darauf, daß es den Umfang der Nutzung seiner Rechte kontrolliert. Beispiel hierfür ist eine Telefonwertkarte, die im Namen der Telefongesellschaft verhindert, daß Gebühreneinheiten mehrfach ausgegeben werden.

2.2 Vertrauensbildende Maßnahmen nach Vertrauensarten

Vertrauen in persönlichen Agenten

- Diese Art von Vertrauen beruht auf der Vertrauenswürdigkeit von Entwurf, Herstellung, Auslieferung, Personalisierung, Initialisierung und gegebenenfalls auch Wartung der Geräte. Obwohl „vertrauenswürdig“ nicht objektiv meßbar ist, existieren Maßnahmen, die diese Vertrauenswürdigkeit erhöhen.
- Eine gut durchdachte und dokumentierte Benutzerschnittstelle ist zwingend notwendig, um dem Benutzer zu ermöglichen, seine Wünsche dem Gerät zu vermitteln. Ein Beispiel ist die Warnfunktion (eine wichtige Funktionen der handgeschriebenen Unterschrift) beim Unterschreiben.

Spezielle Fragestellungen, die wir in späteren Kapiteln wieder aufgreifen, sind:

- Maßnahmen zur Erhöhung des Vertrauens in einen Entwurf — vorrangig Diversität und andere Methoden der Software-Fehlertoleranz (Kap. 3.1).
- Auch wenn die Benutzer dem Entwurf vertrauen, muß garantiert werden, daß die gelieferten Geräte dem Entwurf entsprechen (Kap. 3.2).
- Für alle Beteiligten vertrauenswürdige Erzeugung von Schlüsseln (Kap. 3.3).
- Unter welchen Bedingungen können mehrere Parteien mit gegensätzlichen Sicherheitsanforderungen demselben SM vertrauen (Kap. 3.4)?
- Wie können Benutzer sicher sein, was sie signieren, wenn das Display eines POB eigentlich zu klein ist, um die Dokumente darzustellen (Kap. 4)?

Vertrauen in entführten Agenten

Für diese Vertrauensart wird ein SM benötigt, dem der Benutzer vertraut. Dies kann zugleich das POB sein[4]. Dieses SM sollte

- den Benutzer identifizieren (z.B. durch PIN, Passwort oder Biometrik) und
- geheime Schlüssel speichern und verwenden. Wenn SM und POB nicht identisch sind, gehören dazu die Schlüssel zur Geheimhaltung und Integritätsprüfung von aus dem SM in das ungeschützte POB ausgelagerten Daten.

---

[4] Alternativ könnte der Speicherinhalt des POB mit einem geheimen Schlüssel des Benutzers verschlüsselt werden. Dieser muß nach dem Einschalten eingegeben werden. Kaum ein Benutzer wird jedoch bereit (und fähig) sein, sich einen kryptographisch sicheren Schlüssel zu merken (ein 56-bit DES Schlüssel wäre das Minimum). Im Prinzip könnte man auch Biometrik verwenden, um einen sicheren Schlüssel abzuleiten. Erstens ist jedoch unklar, ob immer derselbe Schlüssel abgeleitet wird. Zweitens gibt es kaum Variationsmöglichkeiten für den Schlüssel (nur 10 Finger …). Drittens könnten auch andere die Schlüssel ableiten (z.B. von Fingerabdrücken an Weingläsern, siehe Kap. 6.1).

Manche POBs können während des Betriebs verloren oder gestohlen werden (z.B. Mobiltelefon). Dies ist problematisch, da ein Angreifer das POB weiter nutzen oder während des Betriebs ausforschen kann. Gegenmaßnahmen teilen sich auf in

- solche, die das Verlustrisiko zu verringern, und
- solche, die den Schaden bei eventuellem Verlust begrenzen.

Analog sollten wartbare POBs einen Wartungsmodus besitzen, in dem sie ohne SM arbeiten. Genauer wird untersucht:

- Welche Bauformen von SMs verringern das Verlustrisiko (Kap. 5)?
- Aspekte der Benutzeridentifikation:
  - Verhindern der Beobachtung wichtiger PINs (Kap. 6.1).
  - Benutzerfreundliche Autorisierung mehrerer Schritte (Kap. 6.1).
  - Schutz vor gefälschten POBs (Kap. 6.2).
- Kosten und Nutzen durch Brechen der sicheren Hardware (Kap. 7.1).
- Für welche Teile eines POB wird sichere Hardware gebraucht (Kap. 7.2)?

Vertrauen in Agenten in feindlicher Umgebung

Dies setzt in der Regel ein SM des zu schützenden Dritten voraus. Diese Art von Vertrauen wird jedoch nicht bei allen Anwendungen benötigt, beispielsweise nicht bei Zahlungssystemen mit Online-Prüfung der Transaktionen [Chau 89].

Im Gegensatz zu den anderen Vertrauensarten ist bei Agenten in feindlicher Umgebung wenigstens die Identifikation zwischen SM und vertretener Person problemlos: Da diese wieder einen Rechner haben kann, können kryptographische Identifikationsprotokolle verwendet werden.

Die einzigen offenen Fragen sind also, wie der Dritte Vertrauen in das SM erlangt und inwieweit der sicheren Hardware vertraut werden kann. Dies wird zusammen mit den entsprechenden Fragen für Vertrauen in entführte Agenten in Kap. 3 und 7 behandelt.

3 Vertrauen ist gut, Kontrolle ist besser

Wodurch kann ein Benutzer einem Gerät vertrauen, das er nicht selbst entworfen und gebaut hat? Natürlich können wir diese Frage nur teilweise beantworten. Auch wenn oft Zertifizierungsinstanzen eingeschaltet werden, beachte man, daß das eigentliche Ziel ist, die Person, deren Sicherheit auf einem Gerät beruht, von der Vertrauenswürdigkeit des Geräts zu überzeugen. Daher sollte sie größtmögliche Kontrolle über Entwicklung und Herstellung des Geräts besitzen.

3.1 Vertrauenswürdige Herstellung

Leider ist Vertrauen in Soft- und Hardware durch Verifikation in der Realität nur in wenigen Spezialfällen machbar. Meist sind nicht einmal prinzipielle Verfahren zur Verifikation der Sicherheit bekannt[5]. Trotzdem kann Vertrauen durch Methoden der Software-Fehlertoleranz erhöht werden.

Strukturierte und modulare Entwicklung

Wie bereits üblich, kann Sicherheit z.B. durch einen kleinen (eventuell sogar beweisbaren) Sicherheitskern unterstützt werden.

Strukturierte und modulare Entwicklung ermöglicht weiterhin Diversität (Mehrfachauslegung von Modulen) auf mehreren Ebenen und erhöht die Abwehrchancen für eventuelle Angriffe.

Qualitätskontrolle von jedem Produktionsschritt

Wie in der Informatik (hoffentlich) üblich und bereits teilweise standardisiert [ITSEC 91], sollten die einzelnen Schritte einer Qualitätskontrolle unterliegen. Die Qualitätskontrolle an sich muß natürlich auch vertrauenswürdig sein. Daher sollten die folgenden Maßnahmen zur Erhöhung des Vertrauens auch auf sie angewendet werden.

Diversität der Produktionsschritte

- *Diversität der Entwicklung:* Die Entwicklung sollte so öffentlich wie möglich sein und von möglichst vielen unabhängigen Experten überprüft werden.[6]
- Für alle Einzelteile und Programme sollten *verschiedene Bezugsquellen* existieren, um die Chance zu erhöhen, daß jeder Benutzer eine für ihn hinreichend vertrauenswürdige Bezugsquelle findet.

Qualitätskontrolle und Diversität sind zum Teil aber gegensätzlich: Bei begrenztem Budget sinkt die Qualität bei zu vielen unabhängigen Entwicklungen.

- Innerhalb eines Geräts wird Diversität wie für die Fehlertoleranz üblich angewendet: Die Grundverfahren Fehlermaskierung[7] und Rücksetzblöcke[8] erhö-

---

5 Es existieren Spezifikationen für manche Komponenten von sicheren Systemen, z.B. Signatursysteme [GoMR 88, Pfit 93] und Authentifikationssysteme [BeRo 94]. Spezifikationen für komplette Systeme (z.B. Zahlungssysteme) existieren jedoch nicht.

6 Die Veröffentlichung der benutzten Algorithmen sollte die Sicherheit eines Systems nicht verringern: Die Sicherheit eines *sicheren* Systems wird durch die Prüfung durch unabhängige Experten bestätigt. Erkennen von *Sicherheitslücken* ermöglicht Abhilfe. Außerdem ist Geheimhaltung sowieso nur schwer möglich: Aufgrund der im Vergleich zu löschbaren Speichern einfacheren physikalischen Auslesbarkeit von ROM können Programme auch bei SMs kaum vor Angreifern geheimgehalten werden.

hen die Verfügbarkeit der Geräte [AnLe 90]. Maskierung verhindert auch verdeckte Kanäle: Übertragung von Information über die Rechenzeit wird verhindert, indem alle Berechnungen nach einer festen Zeit abgebrochen werden (der, die ein korrektes Programm benötigt) [Cles 88]. Beide Lösungen hängen von der Verläßlichkeit der Auswahlkomponente ab. Die Idee ist jedoch, daß diese einfacher zu überprüfen ist als die zu kontrollierenden Komponenten — im Idealfall würde der Benutzer das Ergebnis selbst auswählen.

Sinnvollerweise sollte Diversität auf Logik- und Programmebene angewendet werden, da hier eine vollständige Prüfung nicht möglich ist. Einfachere Hardwarekomponenten, wie physikalische Schnittstellen, wären davon ausgenommen.

Begrenzung der Fehlerausbreitung

Die maximale Auswirkung unverläßlicher Komponenten sollte so beschränkt wie möglich sein. Zur Sicherstellung der Verfügbarkeit und Integrität wird hierzu jede Komponente Plausibilitätskontrollen ihrer Eingaben vornehmen. Selbst kryptographische Kontrolle und Selbstkorrektur von Programmen sind denkbar [BlKa 89]. Zur Sicherstellung der Vertraulichkeit sind die Informationsflüsse auf das absolut Notwendige einzuschränken. Beispiele hierfür sind:

- Datenaustausch zweier Komponenten über einen unsicheren Kanal sollte Ende-zu-Ende verschlüsselt werden. Dies kann bereits nötig sein, wenn ein SM aus mehreren Bausteinen besteht.

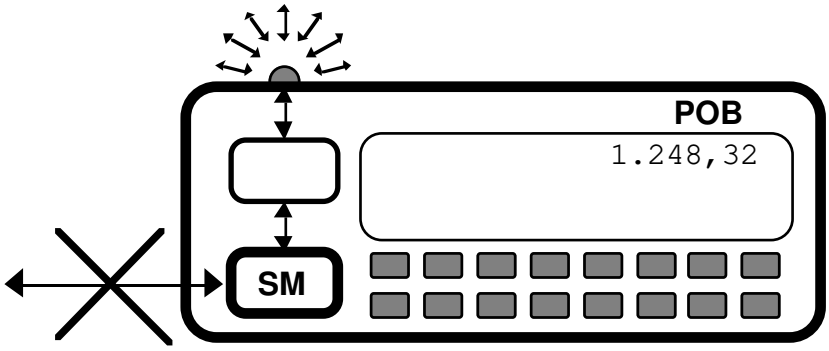

Bild 1: *Unterbindung von Informationsfluß durch ein POB*

- Sollen drei Komponenten *A*, *B*, *C*, so verbunden werden, daß *B* mit *A* und *C,* aber nie *A* direkt mit *C* kommuniziert, so sollte *B* sämtliche verdeckten Kanäle zwischen *A* und *C* schließen (Abb. 1). Dies ist für manche Anwendungen tatsächlich möglich (s. Wallet-Observer-Protokolle [Chau 92, ChPe 93]). Ein einfaches Beispiel ist ein POB *B* mit einem internen SM *A* mit anderem

[7] Auswahl eines Ergebnisses aus einer Menge mehrerer unabhängiger Berechnungen (meist nach der Mehrheit). Dies wird auch *N*-Versionen-Programmierung genannt.

[8] Verschiedene Komponenten versuchen nacheinander ein Ergebnis zu berechnen, bis eine ein korrektes erhält.

Eigentümer, das mit einem externen Terminal *C* kommuniziert.

- Sollen Aufgaben von *A* in eine leistungsfähigere Komponente *B* ausgelagert werden, so sollte *B* möglichst wenig geheime Information erhalten. Hierzu kann *A* das Problem in Teilprobleme zerlegen, diese an *B* weitergeben und die Ergebnisse selbst wieder zusammensetzen [MaKI 90, PfWa 93]. Ebenso kann ein SM verschlüsselte Daten in den unsicheren, aber größeren Speicher des POBs auslagern. (Eine Vergrößerung des SM-Speichers ist vorzuziehen.)

3.2 Original oder Fälschung?

Auch wenn die Entwicklung vertrauenswürdig erscheint, muß noch sichergestellt werden, daß die Geräte dem geprüften Entwurf entsprechen. Viele Fehler und Angriffe könnten durch vollständige Überwachung von Produktion und Auslieferung vermieden werden. Trotzdem sind einige Prüfungen am ausgelieferten Gerät notwendig, die gewisse Angriffe ausschließen:

Auslieferung von verfälschten Geräten

Ein normaler Benutzer kann nur dann feststellen, ob er ein echtes Gerät, d.h. eins vom gewünschten Hersteller, besitzt, falls das Gerät sichere Hardware enthält.[9] Bei hohem Austauschrisiko sollte daher sichere Hardware für alle kritischen Teile (einschließlich Benutzerschnittstelle) eingesetzt werden. Mindestens einfache Erkennungsmerkmale, wie Hologramme, sind immer nötig (Kap. 6.2).

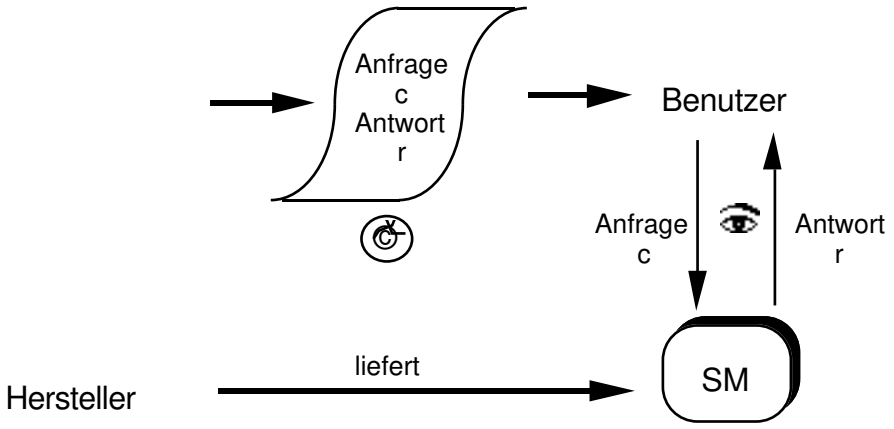

Bild 2: *Frage-Antwort-Mechanismus zur Prüfung der Herkunft des Gerätes.*

Falls das Gerät sichere Hardware besitzt (SM), kann es seine Echtheit durch korrektes Beantworten von Anfragen beweisen. Zum Beispiel kann der Benutzer

---

[9] Umgekehrt erschwert allerdings sichere Hardware unabhängigen Prüfinstanzen das Prüfen zufällig ausgewählter Geräte gegen Fehler direkt vom Hersteller.

direkt vom Hersteller eine zufällige Anfrage *c* und die korrekte Antwort *r* mitgeteilt bekommen und prüfen, ob das Gerät *c* mit *r* beantwortet (Abb. 2). Nach korrekter Antwort sollte dieser Mechanismus außer Kraft gesetzt werden, um unberechtigte Identifizierung durch andere zu verhindern. Alternativ könnte das SM auch vom Benutzer gewählte Nachrichten unterschreiben.

Solche Frage-Antwort-Mechanismen sind nicht sicher, falls ein ausreichender Kanal zwischen dem Angreifer und dem gefälschten POB existiert (z.B. bei Mobiltelefonen): Dann kann das POB die Anfrage an den Angreifer schicken, der sie durch ein korrektes Gerät beantworten läßt (z.B. das entwendete echte) und die Antwort an das gefälschte POB zurückschickt.

Fehlerhafte Geräte direkt vom Hersteller

Dies ist der Fall, wenn das vom Hersteller produzierte Gerät vom geprüften Entwurf abweicht.

Bei getrennt gelieferter Software ist das Problem lösbar, denn sie kann zertifiziert (d.h. durch eine Prüfinstanz elektronisch unterschrieben) werden. Dies setzt allerdings ein anderes hinreichend vertrauenswürdiges Gerät oder eine hinreichend vertrauenswürdige Instanz zur Prüfung der Unterschrift voraus. Das Risiko der Erkennung eines Angriffs ist hier hoch, da die Korrektheit der Unterschrift auch im Nachhinein geprüft werden kann.

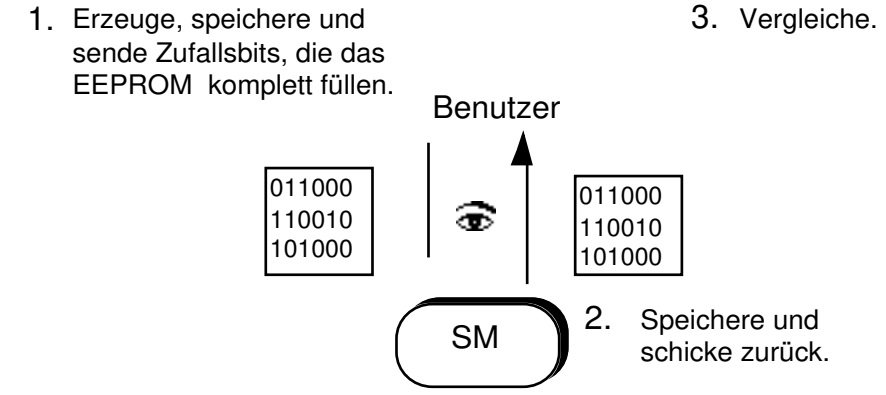

Bild 3: *Sicheres Löschen des EEPROMs.*

Für Programme im ROM und die Logik der Bausteine gibt es keine einfachen Testverfahren, die der Benutzer selbst anwenden kann. Ein Hauptproblem ist der Nachweis, daß keine versteckte Funktionalität existiert, z.B. eine bestimmte zehnstellige Zahl, die das SM zu unerwünschten Aktionen veranlaßt. Einzige Möglichkeit für den Benutzer ist zu prüfen, ob alle gewünschten Funktionen korrekt arbeiten und zu hoffen, daß diese den verfügbaren Platz vollständig ausfüllen. (Parallel dazu können Verbraucherschutzorganisationen natürlich Stichproben weitergehend überprüfen).

Falls das SM zu Beginn kein Geheimnis außer für den oben beschriebenen

Frage-Antwort-Mechanismus enthält und die Speichergröße bekannt ist, kann der Benutzer zumindest das Löschen des Speichers überprüfen (Abb. 3): Der Benutzer sendet zufällige Daten an das SM, die den ganzen Speicher ausfüllen. Anschließend muß das SM genau diese Daten wiedergeben.

Analog kann die Größe von Geheimnissen im EEPROM geprüft werden. Weitere Prüfungen sind möglich, falls die Geheimnisse bekannte Eigenschaften haben sollen. Meist werden jedoch zum Auslieferungszeitpunkt noch keine Geheimnisse (außer evtl. ein Zufallsanteil für die Schlüsselerzeugung, s. unten) im EEPROM gespeichert.

Bei analogen Merkmalen des Geräts treten spezielle Probleme auf:

- Falls individuelle analoge Merkmale auch für andere Geräte sichtbar sind (z.B. Hologramme, Kapazitäten oder Widerstände), lassen sie unerwünschte Identifikation zu.
- Falls sie geheim sind (analoge Maßnahmen, die den Nachbau trotz vollständiger Digitalinformation erschweren), ist dies unverträglich mit den anderen Sicherheitsanforderungen: Diese undokumentierte Funktionalität kann nur durch wenige geprüft werden[10]. In den häufigen Fällen, daß das SM nur durch ein POB oder über ein Netz kommuniziert, sind diese Maßnahmen sowieso ausgeschlossen (Mobiltelefone u.ä.).

3.3 Initialisierung und Schlüsselerzeugung

SMs müssen in der Lage sein, Schlüssel so zu erzeugen, daß Zufälligkeit und Geheimhaltung gesichert ist. Das einzige Problem hieran ist meist die Erzeugung von anfänglichen Zufallsbits.[11] Diese werden entweder direkt in der Schlüsselerzeugung benutzt oder als Startwert eines Pseudozufallszahlengenerators (z.B. zur Erzeugung von Modulus und initialem x des x^2-mod-n-Generators [BlBS 86]).

Falls das SM keinen physikalischen Zufallsgenerator besitzt oder man diesem nicht vollständig vertraut, sollte dem Benutzer gestattet werden, seinen Teil zu der Zufälligkeit beizutragen — Sicherheitsbewußte werden hier zu Münze oder Würfel greifen. Die Erzeugung einer gemeinsamen Zufallszahl aus den einzelnen Zahlen ist bei sicherer und vertrauter Hardware einfach: Jede Gruppe gibt eine Zufallsfolge der gewünschten Länge ein. Das SM verknüpft diese mit XOR. War

---

[10] Man könnte darauf vertrauen, daß diese individuellen Merkmale nur von wenigen Geräten geprüft werden (z.B. von Bankautomaten, nicht jedoch Ladenkassen) oder daß nur allgemeine Merkmale geprüft werden. Beides ist jedoch unbefriedigend, da die Einschränkungen kurzfristig und unbemerkbar aufgehoben werden können.

[11] Der Speicherplatz für Programme zur Schlüsselerzeugung (z.B. erweiterte Primzahltests) ist kein Problem. Falls das SM das Laden von Anwendungen erlaubt, ist dies nur eine Anwendung. Nach Erzeugen der Schlüssel kann diese oft gelöscht und durch andere Anwendungen überschrieben werden.

mindestens eine Eingabe zufällig, so ist das Ergebnis auch zufällig.[12]

3.4 Ein SM als Doppelagent

Wir wollen schließlich untersuchen, wie sinnvoll die Annahme ist, daß mehrere Parteien, meist ein Benutzer und ein Diensterbringer, einem einzigen SM vertrauen (auch bezüglich der Rechtsgültigkeit der gemeinsamen Transaktionen).

Eine zwingende Voraussetzung ist, daß die Sicherheit des SM von keiner dieser Parteien abhängt, d.h. der Hersteller muß von allen unabhängig sein. Die Parteien müssen sich sogar auf sichere Weise gemeinsam auf einen Hersteller einigen (schlimmstenfalls durch gemeinsamen Münzwurf [Blum 83]).

Hauptargumente gegen die Nutzung eines SM durch mehrere Parteien sind:

- Ein solches System ist nicht offen: Zum Beispiel muß bei einem Wechsel der Bank die neue Bank demselben SM wie die vorherige vertrauen. Die Einstellung der Banken hierzu ist unklar: In kleinem, nationalem Rahmen mag dies möglich sein, nicht jedoch für weltweite Anwendungen. (Wieso sollten Banken diese Einschränkungen in Kauf nehmen, wenn Public-Key-Verfahren ihnen erlauben, sich nicht gegenseitig völlig zu vertrauen?)
- Es ist unklar, ob alle Gruppen sich auf ein SM einigen können.

Die Hauptargumente für Doppelagenten-SMs sind Benutzerfreundlichkeit und Kosten. Da POBs jedoch leistungsfähiger sein werden und Einsteck-SMs sowieso verwendet werden, wird der Preis eines SMs im Vergleich zum Gesamtpreis vernachlässigbar sein.

Doppelagenten-SMs müssen in der Lage sein, Schlüssel zu erzeugen, deren Zufälligkeit und Geheimhaltung alle Parteien glauben. Der einzige Unterschied zu Kap. 3.3 ist, daß jede Gruppe einen Zufallsanteil beisteuern muß.

4 POB als Periskop des Benutzers

Wie kann ein Benutzer ein großes zu signierendes Dokument durch eine im Verhältnis hierzu kleine Anzeige eines POB betrachten? Oder, wie kann ein Benutzer eine Zahlung autorisieren, wenn die Anzeige kaum mehr als die Anzeige des Betrages zuläßt? Die Prüfung auf einem größeren Gerät (Workstation) scheidet meist aus, da das POB das einzige verläßliche Gerät ist und andere Geräte somit unterschiedliche Dokumente anzeigen und zur Signatur einreichen könnten [Pord 93, PoRS 93].

Es gibt hierfür keine umfassende Lösung, jedoch einige Ansätze. Man kann frei-

[12] Dies verträgt sich auch mit dem sicheren Löschen des Speichers: Da die Größe der Zufallsfolge bekannt ist, wird sichergestellt, daß alle anderen Teile wirklich leer sind.

formulierte Texte und feste bekannte Formulare (z.B. Überweisungen) unterscheiden. Bei letzteren muß das POB nur die variablen Teile anzeigen.

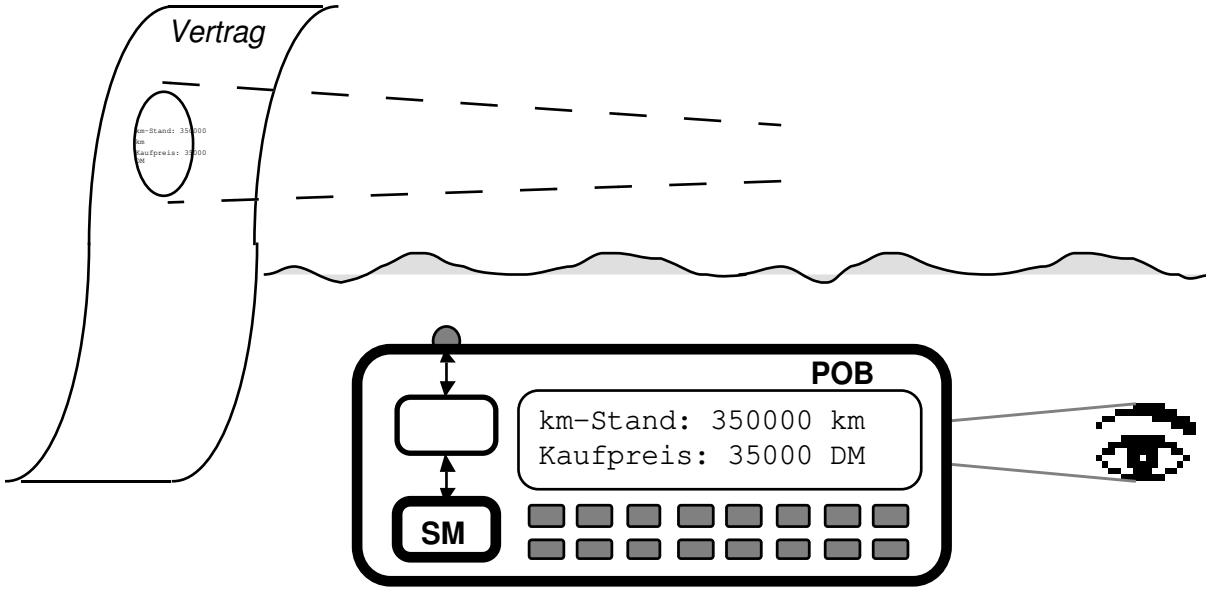

Bild 4: *Betrachten von großen Dokumenten mit kleiner POB-Anzeige*

Verkleinerung des Dokumentumfangs

- Entwickler und Benutzer sollten versuchen, die Gesamtgröße der Dokumente klein zu halten. Dies bedeutet unter anderem das Weglassen von wenig aussagekräftigen Floskeln und anderen nicht rechtsrelevanten Teilen.
- Reduzierung des variablen Teils des Dokuments durch Benutzung von Formularen, falls möglich. Jedes Formular und jedes Feld benötigen eindeutige Namen. Das POB muß Name und Wert jedes Feldes anzeigen können.

POBs mit leistungsfähiger Benutzerausgabe

- Hochauflösende Grafik ermöglicht das Absuchen des Dokuments mit einem Fenster.
- Weitere Ausgabekanäle, wie Sprache, erhöhen die Aufnahmefähigkeit.

Erzwingen des Durchlesens des Dokuments

Falls elektronische Unterschriften eine ähnliche Warnfunktion wie eigenhändige haben sollen, sollte das POB den Benutzer zwingen, das Dokument vollständig anzuschauen. So könnte das POB bei Formularen jeden Feldnamen und -inhalt einige Sekunden anzeigen und einzeln um Bestätigung bitten (oder sogar — für sehr wichtige Werte — das korrekte Abtippen erzwingen).

Für sehr große Dokumente ist dies jedoch zu aufwendig (z.B. bei einem 100-seitigen Vertrag — aber wer liest den schon auf Papier?). Hier könnte das POB zufällige Stichproben anzeigen, die der Benutzer mit einer gedruckten oder

anderweitig angezeigten Version vergleicht, und dem Benutzer zusätzlich ermöglichen, beliebige Teile einzusehen (z.B. den Kaufpreis, der bei einer Zufallsstichprobe nur selten angezeigt würde).

Dieses Verfahren kann nicht ohne weiteres auf nichtlineare Daten, wie Hypertext, übertragen werden. Hypertext sollte jedoch in naher Zukunft nicht für Rechtsgeschäfte verwendet werden, da hier die nötige Warnfunktion kaum realisierbar ist.

Ausgabe auf anderen weitverbreiteten Ausgabegeräten

POBs können zur Ausgabe passive Standardausgabegeräte, wie z.B. Fax, Postscript-Drucker, Fernsehgeräte oder beliebige Computerbildschirme benutzen. Diese Lösung ist nicht optimal, da der Benutzer irgendeinem solchen Gerät vertrauen muß. Vorteile sind jedoch, daß ein derartiges Gerät nahezu immer verfügbar ist und daß durch die hohe Diversität ein Angriff erschwert wird. Auf jeden Fall ist diese Lösung vertrauenswürdiger als die Anzeige über den Bildschirm des Vertragspartners, wird also oft das Mittel der Wahl sein.

Um die Sicherheit dieser Lösung zu erhöhen, könnten Verfahren wie visuelle Verschlüsselung [NaSh 94] entweder direkt (Drucker und konstante Folie mit Schlüssel) oder durch Aufteilung der Daten in mehrere Teile für mehrere Ausgabegeräte eingesetzt werden. (Um eventuelle Fehler zu erkennen, müssen die Dokumente hierbei Redundanz besitzen.)

Andere Anforderungen, die das Unterschreiben von großen Dokumenten an SMs und POBs stellt, sind Übertragungs- und Speicherleistung zur Verarbeitung des gesamten Dokuments.

5 Freiheitserhaltende Maßnahmen für Agenten

In diesem Abschnitt schlagen wir Maßnahmen vor, die das Verlustrisiko vor allem von SMs minimieren.

Falls ein Gerät so klein ist, daß es am Körper getragen werden kann, ist das Verlustrisiko geringer als in Taschen, Mänteln oder gar im Büro[13]. Derzeit ist dies nur für kleine SMs, nicht aber für POBs möglich. (Zusammenrollbare Bildschirme sind noch nicht erhältlich, aber denkbar [Brow 94].) Als Bauarten für solche kleinen herausnehmbaren SMs sind denkbar:

a) Einsteck-SMs: Das SM wird meistens außerhalb des POB aufbewahrt und während des Betriebs in das POB eingesteckt. Das Risiko, POB und SM zusammen zu verlieren, liegt beim Benutzer. Spezielle Aufbewahrungsvorrichtungen für die SMs bestimmen das Verlustrisiko maßgeblich mit.

---

[13] Es sind bereits Uhren mit Tastatur und Infrarotschnittstelle oder Funkrufempfänger erhältlich [Funk1 94, Funk 94].

b) Externe SMs: Das SM ist immer getrennt vom POB und benötigt daher einen Kommunikationskanal zum POB. Funk, Infrarot oder Induktion sind denkbar, beschränken jedoch die Aufbewahrungsmöglichkeiten am Körper. Die Verbindung zwischen POB und SM muß verschlüsselt und authentisiert werden.

Da herausnehmbare SMs nur mit speziellen POBs kommunizieren müssen, gibt es keinen Grund, an ISO-Smartcards festzuhalten. Es gibt heute schon leistungsfähigere Bauarten für 1-Chip Module:

- Mobiltelefonchipkarten (wie ISO-Smartcard, nur auf kleineren Plastikkarten).
- Kleine Edelstahlknöpfe (Aussehen wie Knopfzellen) [Dall 94].
- Schlüsselanhänger, die an einer Kette getragen werden können, vorgesehen zur Speicherung von medizinischen Notfalldaten (z.Zt. bis 128KB) [Plus 90].
- PCMCIA-Module.

Vorteile der letzten drei Bauformen sind erhöhte Bruchsicherheit und Platz für größere oder mehrere Chips. Für die Mobiltelefonchipkarten und die Knöpfe werden spezielle Aufbewahrungsvorrichtungen benötigt.

Mögliche Bauformen für externe SMs oder Aufbewahrungsvorrichtungen sind

- Uhren,
- Halsketten, Ohrringe, Ringe oder anderer Schmuck,
- Anhänger am Schlüsselbund[14].

Von wichtigen Modulen können auch verschiedene Bauformen angeboten werden, so daß wahrscheinlich ist, daß jede und jeder eine geeignete Form findet.

6 Benutzeridentifikation: Freund oder Feind?

In diesem Abschnitt untersuchen wir Besonderheiten von Verfahren zur gegenseitigen Erkennung von Benutzer und POBs. Wir vergleichen nicht verschiedene Identifikationsverfahren, wie PINs, Passwörter und Biometrik, da hierüber bereits ausführliche Abhandlungen existieren [DaPr 89, Fitz 89, Mill 94].

6.1 Benutzeridentifikation

Identifikationszeitpunkte im Idealfall

Als Basis für die weiteren Betrachtungen geben wir an, wann und bei welchen Protokollschritten Benutzeridentifikation im Idealfall (d.h. wenn vollkommen

[14] Normale Leute sollten hierauf sicher immer gut aufpassen — wir scheinen aber wenig normale Leute zu kennen.

sicher und benutzerfreundlich) nötig wäre, um den Schaden bei Verlust (auch im Betrieb) zu minimieren:

- Bei jeder für den Benutzer sicherheitskritischen Aktion:
  - Jede unterschriebene Nachricht, die den Benutzer verpflichtet.
  - Jede Entscheidung zur Weitergabe von persönlichen Daten.

  Falls das Verlustrisiko während des Betriebs als gering eingeschätzt wird, genügt Identifikation beim Anschalten und Bestätigung der einzelnen Aktionen durch ein „OK".
- Will man verhindern, daß ein Gerät längere Zeit unberechtigt in Betrieb bleibt (weil das für die Ausforschungssicherheit nachteilig ist), ist Identifikation in festen Zeitintervallen nötig. Bei aufwendigen Verfahren (PIN, dynamischer Unterschriftvergleich) ist dies aber für die Benutzer kaum akzeptabel.
- Speziell für externe SMs, die direkt am Körper getragen werden, sind billige Identifikationsverfahren denkbar, die zwar den Benutzer nicht sicher erkennen, aber seine ununterbrochene Anwesenheit prüfen (Körpertemperatur, Herzschlagmessung). Dies ist mit einer einmaligen (aufwendigeren) Identifikation durch das POB zu Beginn jeder Transaktion zu kombinieren.

Beobachtbarkeit von Identifikation und Risikoklassen von Eingaben

Die meisten Identifikationsarten können von Angreifern beobachtet werden:

- Zuschauen bei der PIN-Eingabe.
- Fingerabdrücke auf Gläsern.
- Messung der Tastaturabstrahlungen während der PIN-Eingabe.
- Dynamische Aufzeichnung von handgeschriebenen Unterschriften durch Paketdienste [UPS 94].

Die Beobachtbarkeit kann eingeschränkt, aber nicht ausgeschlossen werden.[15] Daher wird eine Risikoanalyse benötigt, die Nutzen und Aufwand einer Beobachtung vergleicht. (Ein Ergebnis ist z.B., die Zahlungs-PIN nicht zum Abheben zuzulassen.) Die Benutzereingaben werden dann in Risikoklassen eingeteilt.

- Für verschiedene Risikoklassen sollten verschiedene Identifikationsverfahren gewählt werden können.
- Bei PINs sollten Benutzer, die sich nur eine merken können, diese ausschließlich für Eingaben der höchsten Risikoklasse benutzen.
- Selbst eine triviale PIN (solange sie unabhängig von der Hochsicherheits-PIN

---

[15] Ein Vorschlag sind variable PINs. Hier ist jede einzelne Beobachtung wertlos. Die Autoren gestehen jedoch ein, daß dies für die meisten Benutzer zu kompliziert wäre [MaIm 91].

ist) für eine niedrigere Risikoklasse ist besser als keine, da sie den erwarteten Nutzen bei Diebstahl verringert.

- Es sollte eine Möglichkeit geben, die nötige Identifikation vor dem Ereignis durchzuführen[16]. Die kritische Aktion wird dann nur durch ein OK bestätigt (z.B. Freigeben des Betrages im Auto statt in der Schlange an der Kasse der Tankstelle, Bestätigung an der Kasse nur durch „OK“). Das OK ist nötig, da sonst der Vertragspartner unbemerkt beliebige Aktionen durchführen kann.

Benutzerfreundlichkeit

Die Häufigkeit der Identifikation und die Wahl des Verfahrens ist immer ein Kompromiß zwischen Benutzerfreundlichkeit und Sicherheit. Die Entscheidung sollte jedoch weitgehend dem Benutzer überlassen werden und situationsabhängig möglich sein. Um eine sachgerechte Wahl zu ermöglichen, sind Warnungen und geeignete Vorgabewerte hilfreich.

Schlußbemerkungen

Denkbar wäre auch eine Notfall-PIN, die nur unter Zwang gebraucht wird: Transaktionen mit ihr sehen gültig aus, sind aber nichtig.

Da jedoch vielerlei Probleme bei der Identifikation auftreten, halten wir es für nötig, Transaktionen von hohem Wert durch Notare beglaubigen zu lassen.

6.2 Schutz vor gefälschten POBs

Bisher haben wir die Identifikation des Benutzers durch das Gerät behandelt. Auch für die Identifikation des Geräts durch den Benutzer existieren unterschiedliche Möglichkeiten:

- Die Standardmethode sind physikalische Merkmale wie Hologramme oder eingeschweißte Fotos, die vom Benutzer direkt erkannt werden können. Aus Datenschutzgründen sollte eine automatische Identifikation des Geräts durch Dritte allerdings nicht möglich sein. (Eingeprägte Nummern z.B. könnten leicht abgelesen werden.)
- Die Benutzung von Geräteidentifikationsnummern (DIN, *device identification number*) hilft wenig oder ist zu kompliziert. Eine feste Nummer ist nutzlos, da sie einen derartigen Angriff nicht verhindert. Jeweils nur einmal verwendete Paare (DIN, PIN) von Gerät- und Benutzeridentifikationsnummern sind denkbar. Da Listen mit diesen Paaren aber schriftlich vorliegen müßten, ist die Anwendbarkeit eingeschränkt.

---

[16] Bei dieser Gelegenheit kann der Benutzer eine kurze Einmal-PIN erhalten, die er dann anstelle des OK eingibt.

- Falls der Benutzer ein weiteres Gerät besitzt, können kryptographische Verfahren eingesetzt werden. Z.B. kann für POBs mit internem Smartcardleser dieses zweite Gerät eine Smartcard sein. Während der Initialisierung erhält sie eine spezielle Nummer (DIN) vom Benutzer. Wenn die Smartcard das POB identifiziert hat, gibt sie (da sie keinen eigenen Ausgabekanal zum Benutzer hat) diese DIN über das POB aus. Der Benutzer gibt nur bei korrekter DIN seine PIN ein. Anschließend wird die Smartcard entnommen.

  Bei Benutzung eines externen SMs, das ein Benutzer immer am Körper trägt, kann dies auch zur Identifikation anderer POBs und SMs eingesetzt werden.

  In beiden Fällen ist noch der oben beschriebene Angriff durch ein POB, das die Anfragen an den Angreifer weiterleitet und von diesem die Antworten eines korrekten POBs erhält, möglich. Dies kann nur verhindert werden, indem unerwünschte Kommunikation des POBs physisch unterbunden oder die physische Nähe des antwortenden POBs geprüft wird (Abstandsbegrenzungsprotokoll [BrCh 94]).

Die Verfahren können kombiniert werden: sichere Identifikation mit Smartcard nach Verleih/Wartung und weniger sichere mit Hologramm bei jeder Benutzung.

7 Das Schutzschild des Agenten

Wir betrachten nun den physischen Schutz der Hardware vor Veränderung und Ausforschung. Benötigt wird dieser für entführte Agenten und Agenten in feindlicher Umgebung. Größter Unterschied ist, daß ein Agent in feindlicher Umgebung voll funktionsfähig bleiben soll, ein entführter Agent jedoch nur gegenseitige Identifikation zulassen soll (abgesehen vom Verlust während des Betriebes, siehe Kap. 6.1). Schlägt sie fehl, sollten keine weiteren Operationen möglich sein.[17]

7.1 Risikoabschätzung

Der Schutzgrad von sicherer Hardware ist nicht genau meßbar. Sicher gibt es keinen absoluten Schutz gegen Angreifer mit ausreichend Wissen, Zeit und Ausrüstung. Daher ist eine Risikoabschätzung nötig: Der Aufwand, ein Gerät zu brechen und die Wahrscheinlichkeit, daß dies erkannt wird, sollten in ausgewogenem Verhältnis zum erzielbaren Gewinn stehen.

Nach Artikeln wie [Krus 91, Pate 91] ist zu vermuten, daß zum Brechen ein gut ausgestattetes Labor und ein fester Mehraufwand je gebrochenem Gerät nötig

---

[17] Ein entführter Agent muß auch mindestens eine geheime PIN o.ä. speichern. Die Beobachtungsmöglichkeiten bei der PIN-Prüfung lassen sich jedoch durch Speichern der einzelnen Bits an verschiedenen Stellen und sukzessiven Vergleich der einzelnen Bits verringern.

ist. Damit könnte eine konkrete Risikoabschätzung so aussehen:

- Berauben von Benutzern bei geringen Werten: Bei einem off-line Zahlungssystem mit
  - einem niedrigen Höchstbetrag auf der Karte,
  - ohne oder mit begrenzten on-line Abhebungen vom Konto und
  - eventuell Maßnahmen zur Erkennung von Abhebungen mit gestohlenen Karten

  ist das Risiko, daß eine Karte gestohlen wird und die PIN durch Brechen des Geräts ausgelesen wird, relativ gering, da das Beobachten der PIN weitaus weniger Aufwand erfordert.
- Berauben von Benutzern bei hohen Werten: Bei Home-Banking mit großen Beträgen oder bei elektronischen Unterschriften kann sich das Brechen des physischen Schutzes lohnen.
- Bankraub: Das vollständige Brechen eines Systems verspricht nahezu unabhängig vom nötigen Aufwand hohe Gewinne auf Kosten der Bank. Daher sollte die Bank ein Zahlungssystem mit einzeln elektronisch unterschriebenen Münzen verwenden, da hier Betrug sofort und sicher erkannt und lokalisiert werden kann, ohne auf Datenschutz verzichten zu müssen [ChFN 90, FrYu 93, Bran 94, Ferg 94].
- Datenschutz: Das Brechen eines SMs, um Daten des Benutzers auszuforschen, wird sich im allgemeinen nicht lohnen. (Allerdings sollten die Daten nicht in völlig ungeschützten Geräten gespeichert werden.) Geheimdienste könnten jedoch Geräte in Einzelfällen brechen, um die bisherigen Aktionen des SMs nachvollziehen zu können (z.B. durch Auslesen eines Schlüssels und Aufdecken der Daten der Bank).

7.2 Entwurfsentscheidungen

Folgende Punkte sollten während des Entwurfes von sicherer Hardware berücksichtigt werden:

Schutz von Schnittstellen

Für gewisse Anwendungen sollte die Benutzerschnittstelle Teil des SMs sein (d.h. das POB ist ein SM). Andernfalls sind Angriffe durch vertauschte Geräte möglich und kaum festzustellen. Denkbar sind das Abfangen einer PIN über eine vertauschte Tastatur, das Verändern der Tastaturbelegung (Ja/Nein-Tausch) oder das Verändern der Anzeige (Anzeige zu kleiner Beträge). Angriffe dieser Art werden sicher vorkommen, insbesondere gegen besonders arglose Benutzer. Meist wird es aber einfachere Angriffsformen geben, etwa die direkte Beobachtung der PIN-Eingabe oder, für Massenbetrug, der besonders „günstige“ Verkauf

manipulierter Ein-/Ausgabegeräte an möglichst viele Benutzer.

Speicherarten

Verschiedene Speicherarten besitzen unterschiedliche Schutzgrade:

- ROM: Das Auslesen von ROM durch spezialisierte Angreifer ist kaum verhinderbar. Daher darf die Sicherheit weder auf geheimen Schlüsseln noch auf geheimen Verfahren im ROM beruhen.
- Daten in Schreib-/Lesespeichern (z.B. EEPROM oder batteriegepuffertes RAM) von batteriegespeisten Geräten können bei einem Angriff gelöscht werden. Kritisch ist hier nur die Zeit des Löschens. Batteriegepuffertes RAM ist daher am geeignetsten. Dies spricht für SMs, die größer sind als eine Prozessorchipkarte.

Verlust im Betrieb

Das Gerät sollte sich automatisch abschalten, falls es längere Zeit nicht benutzt wurde oder falls eine Aktion abgeschlossen wurde. Außerdem sollte nicht auf geheime Daten zugegriffen werden, falls nicht kurz zuvor eine Identifikation stattgefunden hat (siehe auch Fußnote 17).

Sonstige

Viele Anwendungen benötigen verläßliche Zeitgeber (evtl. sogar Echtzeit) oder physikalische Zufallsgeneratoren. Ein universell einsetzbares SM sollte diese Funktionalität besitzen.

8 Fazit

Die ersten Abschnitte gaben einen Überblick über Vertrauensarten und vertrauensbildende Maßnahmen für portable Benutzerendgeräte und Sicherheitsmodule. Anschließend wurden spezielle Aspekte betrachtet:

- Vertrauen in Geräte kann nie vollständig gerechtfertigt werden. Man kann nur versuchen, möglichst viele vertrauensbildende Maßnahmen anzuwenden.
- Jedes Dokument, das von einem POB unterschrieben werden soll, muß durch den Benutzer über eine vertrauenswürdige Benutzerschnittstelle komplett autorisiert werden. Es wurde gezeigt, wie dies auch mit eingeschränkten Ausgabemöglichkeiten möglich ist.
- Bei Verwendung von ausforschungssicherer Hardware sollte das komplette POB und nicht nur einige Teile geschützt werden. Wichtig ist hierbei die Vertrauenswürdigkeit der Benutzerschnittstelle. Werden Rechte mehrerer Parteien verwaltet, so ist pro Partei ein SM sinnvoll.

- Es wurde gezeigt, daß Sicherheit und Benutzerfreundlichkeit vereint werden können, z.B. durch verschiedene Identifikationsverfahren für unterschiedliche Sicherheitsstufen und Auswahl durch den Benutzer.

Abschließend sei angemerkt, daß die derzeitige Entwicklung von vielen unterschiedlichen POBs auch für sicherheitskritische Anwendungen vorteilhaft ist. Da zur Zeit noch keine vertrauenswürdigen ausforschungssicheren POBs zur Verfügung stehen, ist es derzeit sinnvoll, auf weniger sichere Geräte, die jedoch von vielen Herstellern angeboten werden, auszuweichen und diese durch SMs zu ergänzen. Die meisten dieser Geräte sind leistungsfähiger, benutzerfreundlicher und vielseitiger als spezielle Sicherheitshardware. Die Entwicklung von sicheren Anwendungen sollte sich hauptsächlich auf Protokolle und Verfahren konzentrieren. Die Akzeptanz wird am größten sein, wenn die sicherheitsrelevanten Teile dieser Protokolle in SMs für zielgruppengerechte POBs vertrieben werden, z.B. PDAs oder Mobiltelefone für Manager, Uhren für Computerfeinde und Gameboys für Kinder.

Wir danken *Arnd Weber* vom Institut für Sozialforschung der Universität Frankfurt/M. für zahlreiche Diskussionen und Anregungen.

Literaturverzeichnis

AnLe 90 P. A. Lee, T. Anderson: Fault Tolerance - Principles and Practice; 2nd rev. ed., Dependable Computing and Fault-Tolerant Systems Vol. 3, Springer-Verlag, Wien 1990.

BBCM 94 J.-P. Boly, A. Bosselaers, R. Cramer, R. Michelsen, S. Mjølsnes, F. Muller, T. Pedersen, B. Pfitzmann, P. de Rooij, B. Schoenmakers, M. Schunter, L. Vallèe, M. Waidner: The ESPRIT Project CAFE — High Security Digital Payment Systems; ESORICS 94, LNCS 875, Springer-Verlag, Berlin 1994, 217-230.

BeRo 94 M. Bellare, Ph. Rogaway: Entity Authentication and Key Distribution; Crypto ’93, LNCS 773, Springer-Verlag, Berlin 1994, 232-249.

BlBS 86 L. Blum, M. Blum, M. Shub: A Simple Unpredictable Pseudo-Random Number Generator; SIAM J. Comput. 15/2 (1986) 364-383.

BlKa 89 M. Blum, S. Kannan: Designing Programs that Check their Work; 21st STOC, ACM, New York 1989, 86-97.

Blum 83 M. Blum: Coin Flipping By Telephone, A Protocol for Solving Impossible Problems; ACM SIGACT News 15/1 (1983) 23-27.

Bran 94 S. Brands: Untraceable Off-line Cash in Wallets with Observers;

Crypto ’93, LNCS 773, Springer-Verlag, Berlin 1994, 302-318.

BrCh 94 S. Brands, D. Chaum: Distance-Bounding Protocols; Eurocrypt ’93, LNCS 765, Springer-Verlag, Berlin 1994, 344-359.

Brow 94 J. Brown: Roll up for the flexible transistor, New Scientist 143/1944 (1994), 5.

Chau 89 D. Chaum: Privacy Protected Payments – Unconditional Payer and/or Payee Untraceability; SMART CARD 2000, North-Holland 1989, 69-93.

Chau 92 D. Chaum: Achieving Electronic Privacy; Scientific American (August 1992) 96-101.

ChFN 90 D. Chaum, A. Fiat, M. Naor: Untraceable Electronic Cash; Crypto ’88, LNCS 403, Springer-Verlag, Berlin 1990, 319-327.

ChPe 93 D. Chaum, T. P. Pedersen: Wallet Databases with Observers; Crypto ’92, LNCS 740, Springer Verlag, Berlin 1993, 89-105.

Cles 88 W. Clesle: Schutz auch vor Herstellern und Betreibern von Informationssystemen; Diplomarbeit, Institut für Rechnerentwurf und Fehlertoleranz, Universität Karlsruhe, Juni 1988.

Dall 94 Software Authorization Buttons by Dallas Semiconductors Inc., Werbung, BYTE 8 (1994).

DaPr 89 D. Davies, W. L. Price: Security for Computer Networks (2nd ed.); John Wiley & Sons, New York 1989.

ETSI 90 ETSI/PT12: ETSI/TC GSM 11.11 Specification of the SIM-ME Interface; Version 3.3.0, April 1990.

Ferg 94 N. Ferguson: Single Term Off-Line Coins; Eurocrypt ’93, LNCS 765, Springer-Verlag, Berlin 1994, 318-328.

Fitz 89 K. Fitzgerald: The quest for intruder-proof computer systems; IEEE spectrum 26/8 (1989) 22-26.

FrYu 93 M. Franklin, M. Yung: Secure and Efficient Off-Line Digital Money; 20th ICALP, LNCS 700, Springer-Verlag, Berlin 1993, 265-276.

Funk 94 Funkruf-Trends: Pager für alle; Funkschau 13 (1994) 16.

Funk1 94 Funkruf-Trends: Aus dem Handgelenk (Multitalent); Funkschau 14 (1994) 74.

GoMR 88 S. Goldwasser, S. Micali, R. Rivest: A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks; SIAM J. Comput. 17/2 (1988) 281-308.

GuUQ 92 L. Guillou, M. Ugon, J.-J. Quisquater: The Smart Card: A Standardized Security Device Dedicated to Public Cryptology; in: G. J. Simmons: Contemporary Cryptology – The Science of Information

Integrity; IEEE Press, Hoes Lane 1992, 561-613.

ITSEC 91 Office for Official Publications of the European Communities: ITSEC: Information Technology Security Evaluation Criteria, Version 1.2, Luxembourg 1991 (ISBN 92-826-3004-8).

Krus 91 D. Kruse: The new Siemens computer card; Smart Card 2000, North-Holland, Amsterdam 1991, 3-7.

MaKI 90 T. Matsumoto, K. Kato, H. Imai: Speeding up Secret Computations with Insecure Auxiliary Devices; Crypto '88, LNCS 403, Springer-Verlag, Berlin 1990, 497-506.

MaIm 91 T. Matsumoto, H. Imai: Human Identification Through Insecure Channel; Eurocrypt '91, LNCS 547, Springer-Verlag, Berlin 1991, 409-421.

MeMä 94 R. Mertens, N. Mäthner: Mobilfunk für Verkehrstelematik – System zur automatischen Gebührenerhebung mittels GSM-Mobilfunk; Elektronik 17 (1994) 50-60.

Mill 94 B. Miller: Vital signs of identity; IEEE spectrum 31/2 (1994) 22-30.

NaSh 94 M. Naor, A. Shamir: Visual Cryptography; Pre-proceeding of EUROCRYPT '94, May 9-12, 1994, Perugia, 1-11.

Palm 92 E. Palmer: An Introduction to Citadel – A Secure Crypto Coprocessor for Workstations; IBM Research Report RC 18373 (80423) 9/25/92, IBM Research Division, T. J. Watson Research Center 1992.

Pate 91 M. Paterson: Secure single chip microcomputer manufacture; Smart Card 2000, North-Holland, Amsterdam 1991, 29-37.

Pfit 93 B. Pfitzmann: Sorting Out Signature Schemes; 1st ACM Conference on Computer and Communications Security, acm press 1993, 74-85.

PfWa 93 B. Pfitzmann, M. Waidner: Attacks on protocols for server-aided RSA computation; Eurocrypt '92, LNCS 658, Springer-Verlag, Berlin 1993, 153-162.

Plus 90 PlusTag2 Broschüre, Plus 5 Engineering Limited, Crowborough, East Sussex, UK 1990.

Pord 93 U. Pordesch: Risiken elektronischer Signaturverfahren; Datenschutz und Datensicherung DuD 17/10 (1993) 561-569.

PoRS 93 U. Pordesch, A. Roßnagel, M. Schneider: Erprobung sicherheits- und datenschutzrelevanter Informationstechniken mit Simulationsstudien; Datenschutz und Datensicherung DuD 17/9 (1993) 491-497.

Rolf 94 R. Rolfe: Here Comes Electronic Cash; Credit Card Management Europe, January/February 1994, 16-20.

UPS 94 UPS Signature Pad, Werbung, Der Spiegel 22 (1994) 66-67.