8 Ausblick

8.1 Zusammenfassung

Diese Arbeit hatte zum Ziel, die Sicherheit im elektronischen Zahlungsverkehr zu erhöhen. Um dieses Ziel zu erreichen, wurde ein neues Rollen- und Aufgabenbasiertes Sicherheitsmodell (R&A-Modell) entwickelt, das mit multifunktionalen Chipkarten im elektronischen Zahlungsverkehr realisiert werden kann. Dieses R&A-Modell stellt einen innovativen Schritt über die bereits existierenden Sicherheitsmodelle hinaus dar.

Bei der Entwicklung des Sicherheitsmodells wurde darauf geachtet, daß für den Benutzer kein Administrationsaufwand entsteht, da Benutzerrollen von Administrationsrollen getrennt sind. Die Kombination eines Sicherheitsmodells mit Chipkarten und dessen praktische Anwendung wurde in der Literatur bisher nicht erörtert. Im Hinblick auf die technische Entwicklung von Chipkarten und deren Anwendungsgebieten wird der Einsatz von Sicherheitsmodellen, die in Chipkarten integriert werden, jedoch unbedingt notwendig werden. Mit dieser Arbeit wurde ein wesentlicher Schritt in diese Richtung geleistet.

Zu Beginn der Arbeit wurde die Situation des elektronischen Zahlungsverkehrs, besonders die Entwicklung des karten- und netzgestützten Zahlungsverkehrs untersucht (siehe Kapitel 2.3). Es wurde herausgearbeitet, daß unterschiedliche Zahlungsverfahren sehr unterschiedliche Sicherheitsanforderungen an Vertraulichkeit, Anonymität, Integrität, Verläßlichkeit, Zurechenbarkeit, informationeller Selbstbestimmung und einfacher Handhabung stellen. Dabei wurde speziell auf die Bedürfnisse und Sicherheitsanforderungen von Benutzern im elektronischen Zahlungsverkehr eingegangen.

Die Entwicklung unterschiedlicher Zahlungsverfahren bis heute wurde beleuchtet, und es wurde auf zwei mögliche Trends hingewiesen (siehe Kapitel 2.5). Der eine Trend beschreibt die Entwicklung von vielen inhomogenen Zahlungssystemen, die meist auf je einer Chipkarte basieren. Der zweite Trend beschreibt die Kombination verschiedener Zahlungsverfahren auf einer einzigen multifunktionalen Chipkarte und wurde als Basis für weitere Überlegungen verwendet.

Da das Sicherheitsmodell in erster Linie für die Anwendung auf multifunktionalen Chipkarten entwickelt wurde, wurde zunächst die Technologie der Chipkarten beleuchtet. Es wurde die Funktionsweise und der Aufbau von Chipkarten beschrieben (siehe Kapitel 3), ebenso die Funktionsweise von bekannten Chipkarten-Betriebssystemen (siehe Kapitel 3.5). Weiterhin wurden die Grundlagen von kryptographischen Algorithmen erläutert (siehe Kapitel 4), die in Chipkarten Verwendung finden können. Das R&A-Modell kann auf der Basis von Chipkarten realisiert werden. Es ist jedoch auch möglich, das Sicherheitsmodell auf einer größeren Rechenanlage zu realisieren.

Bevor die Entscheidung über die Entwicklung eines spezifischen Sicherheitsmodells getroffen wurde, wurden bereits bekannte Sicherheitsmodelle vorgestellt und daraufhin

überprüft, ob sie für die gestellten Anforderungen in Frage kommen (siehe Kapitel 5). Dazu wurden, neben den klassischen Zugriffskontrollkonzepten wie DAC und MAC, das Vertraulichkeitsmodell von Bell und LaPadula und das Integritätsmodell von Clark und Wilson vorgestellt. Weiterhin wurden ein Telekooperationsmodell, ein formales Datenschutzmodell und ein Rollenmodell erläutert und anschließend bewertet. Das Ergebnis der Bewertung zeigt, daß keines der vorgestellten Sicherheitsmodelle, wegen ihrer Eindimensionalität (entweder Rollen oder Aufgaben), die gestellten Anforderungen zufriedenstellend erfüllt. Deshalb wurde ein neues, spezifisches Sicherheitsmodell mit zwei Dimensionen entwickelt (Rollen und Aufgaben).

Das spezifische Sicherheitsmodell stellt Rollen und Aufgaben für Benutzer zur Verfügung (siehe Kapitel 6). Die Aufgaben beschreiben, ***was*** ein Benutzer tun kann, während Rollen beschreiben, ***wie*** ein Benutzer eine Aufgabe erledigen kann. Aufgaben können in verschiedenen Rollen erledigt werden. Es existieren eine Menge von Aufgaben und eine Menge von Rollen, die für unterschiedliche Benutzer auf vielfältige Art und Weise miteinander kombiniert werden können. Jede Kombination von Rollen und Aufgaben entspricht einer konkreten Zugriffsmöglichkeit auf vorhandene Datenobjekte. Die Rollen-Aufgaben-Kombination beschreibt weiterhin, welche Information über den Benutzer freigegeben werden darf und auf welche Ressourcen zugegriffen werden darf. Jede Rollen-Aufgaben-Kombination definiert dadurch ein spezifisches Sicherheitsniveau, das durch die Wahl der Kombination von Rollen und Aufgaben realisiert wird. Durch die Kombinationsmöglichkeit der Elemente dieser zwei unabhängigen Mengen ergibt sich eine feine Granularität in der Realisierung des spezifischen Sicherheitsniveau. Die Sicherheit auf Benutzerseite kann dadurch wesentlich erhöht werden.

Das R&A-Modell unterstützt das Prinzip der Pflichtentrennung (separation of duty). Dieses Prinzip hat einen statischen und einen dynamischen Anteil. Die statische Trennung von Pflichten definiert, welche Rollen und Aufgaben für welche Benutzer autorisiert sind. Die dynamische Trennung von Pflichten definiert, welche Rollen-Aufgaben-Kombinationen zur selben Zeit ausgeführt werden dürfen, ohne Konflikte zu erzeugen. Dieses Konzept erlaubt eine gleichzeitige konfliktfreie Ausführung von Anwendungen. Die konfliktfreie gleichzeitige Ausführung existiert für elektronische Zahlungssysteme bisher noch nicht. Ist dies jedoch möglich, ergeben sich vielfältige neue Möglichkeiten in der Gestaltung des elektronischen Zahlungsverkehrs, wobei die Sicherheit für den Benutzer an erster Stelle stehen muß.

Das Sicherheitsmodell wurde in Form eines Zustandsautomaten formal definiert (siehe Kapitel 6.4). Es wurden die Zustandsvariablen beschrieben. Weiterhin wurden Regeln beschrieben, die in den einzelnen Zuständen gelten und Überführungsfunktionen definiert, die von einem Zustand in den nächsten überführen. Die formale Definition wurde in einer formalen Beweisskizze fortgeführt. Es wurde ausführlich die Beweisidee des Zustandsautomaten diskutiert, die im Anschluß skizziert wurde. Ein vollständiger Beweis ist nur dann notwendig, wenn die sichere Implementierung des R&A-Modells gewährleistet werden soll. Eine sichere Implementierung setzt sichere, also bewiesene, Betriebssysteme voraus. Im Chipkartenbereich gibt es zur Zeit jedoch keine formal bewiesenen Betriebssysteme. Aus diesem Grund kann eine sichere Implementierung

nicht garantiert werden. Es gibt bisher nur Chipkarten-Betriebssysteme, die nach ITSEC in der Stufe E4 zertifiziert wurden. Stufe E4 fordert jedoch keinen formalen Beweis der Software, sondern nur deren Spezifikation. Aus diesem Grund ist der hier skizzierte Beweis völlig ausreichend für die vorliegende und für weiterführende Arbeiten.

Bisher bekannte Sicherheitsmodelle sind in der Literatur vorwiegend informell beschrieben oder formal in Form von Zustandsautomaten. Zusätzlich zur Darstellung als Zustandsautomat und der Beweisskizze wurde das R&A-Modell auch als gefärbtes Petrinetz beschrieben (siehe Kapitel 6.5). Petrinetze erlauben in ihrer graphischen Darstellung eine komplexe Darstellungsweise des zugrundeliegenden R&A-Modells. Konflikte und Widersprüche in Systemen können mit der speziellen graphischen Repräsentation von Petrinetzen erkannt werden. Weiterhin konnten Nebenläufigkeiten im R&A-Modell dargestellt werden.

Eine Bewertung des R&A-Modells führt zu folgenden Sicherheitsaussagen (siehe Kapitel 6.6):

- Freie Wahl von Rollen und Aufgaben durch zweidimensionale Struktur
- Feine Granularität der Zugriffe
- Zugriff über wohldefinierte Prozeduren auf Objekte
- Gleichzeitige Ausführung von konfliktfreien Anwendungen
- Statische und dynamische Trennung von Pflichten
- Minimierung der notwendigen Rechte
- Vertraulichkeit und Integrität
- Zugriffsrechte nach MAC und DAC
- Leichte Administration
- Erhöhung der Akzeptanz

Das Sicherheitsmodell erfordert eine aktive Beteiligung des Benutzers. Durch die Wahl einer Rolle und einer Aufgabe kann der Benutzer selbst entscheiden, was er erledigen möchte und welche Informationen er dafür freigeben muß. Um die Benutzung und die Autorisierung der einzelnen Rollen und Aufgaben zu verdeutlichen, wurde nach der Definition des R&A-Modells ein Anwendungsbeispiel des R&A-Modells beschrieben (siehe Kapitel 7). Dabei wurde eine Anwendung einer multifunktionalen Chipkarte modelliert, die unterschiedliche Zahlungs- und Bankfunktionen auf einer Chipkarte erlaubt.

Das Anwendungsbeispiel unterscheidet einen statischen und einen dynamischen Aspekt. Der statische Aspekt beschreibt, daß die einzelnen Rollen, Aufgaben und Rollen-Aufgaben-Kombinationen für die jeweiligen Benutzer autorisiert sein müssen. Er beschreibt weiterhin, welche Rollen und Aufgaben sich gegenseitig ausschließen, um die Anforderungen an das Prinzip der statischen Trennung von Pflichten zu erfüllen.

Der dynamische Aspekt beschreibt beispielhaft eine Benutzung einer multifunktionalen Chipkarte im elektronischen Zahlungsverkehr. Sollen zwei oder mehr Rollen-Aufgaben-Kombinationen gleichzeitig ausgeführt werden, wird überprüft, ob das Prinzip der dynamischen Trennung von Pflichten verletzt wird und sich diese Kombinationen somit gegenseitig ausschließen.

In dem vorgestellten Anwendungsbeispiel waren alle Anwendungen mit ihren Rollen und Aufgaben von vorn herein bekannt und waren zu Beginn der Benutzung definiert. Ein Problem kann dann auftauchen, wenn zu einem späteren Zeitpunkt weitere Anwendungen zu bereits aktiven Anwendungen hinzu geladen werden sollen (siehe Kapitel 3.4). Es muß sichergestellt werden, daß die Anwendungen authentisch sind und die Funktionalität haben, die beschrieben wurde. Ein Ansatz für die Lösung des Problems können Zertifikate für Anwendungen sein, die nicht nur die Echtheit der Anwendung bestätigen, sondern auch eine nachprüfbare Funktionsbeschreibung enthalten.

Eine praktische Implementierung des R&A-Modells auf Basis einer multifunktionalen Chipkarte hätte den Rahmen dieser Arbeit gesprengt. Im folgenden werden interessante und sinnvolle Aufgaben beschrieben, die als Fortführung dieser Arbeit gesehen werden.

8.2 Weiterführende Aufgaben

Um das R&A-Modell auf einer multifunktionalen Chipkarte in einer konkreten Anwendung zu realisieren, müssen zunächst alle Rollen und Aufgaben in dieser Anwendung genau spezifiziert werden. Dies wurde in Kapitel 7 bereits getan. Weiterhin müssen alle Zugriffe, die sich aus den einzelnen Rollen-Aufgaben-Kombinationen ergeben, definiert werden. Aus der Anzahl der Rollen, Aufgaben und Zugriffe ergeben sich Anforderungen an die zugrundeliegende Chipkarte bezüglich Speicherplatz und Prozessorleistung. Wegen Speicherplatzmangel oder zu geringer Prozessorleistung kann in der Konzeptionierung der Anwendung die flexible Kombination von Rollen und Aufgaben eingeschränkt werden. So kann es sinnvoll sein, die gleichzeitige Ausführung von mehreren Rollen-Aufgaben-Kombinationen zu unterbinden. Das R&A-Modell stellt jedoch prinzipiell die volle, maximal flexible Funktionalität zur Verfügung.

Nach Wahl einer geeigneten Chipkarte, kann das R&A-Modell in das Chipkarten-Betriebssystem integriert werden. Dabei ist prinzipiell zu unterscheiden, ob Chipkarten mit „klassischen“ Betriebssystemen wie STARCOS (siehe Kapitel 3.5.6) oder „neue“ Chipkarten mit Java verwendet werden (siehe Kapitel 3.5.7).

Die starre Datenstruktur von STARCOS stellt bei der Integration des R&A-Modells in dieses Betriebssystem eine wesentliche Einschränkung dar. Die Datenstruktur erlaubt keine unterschiedlichen Zugriffe auf dieselben Daten eines Benutzers in verschiedenen Rollen. Der nötige Aufwand, um das R&A-Modell in STARCOS zu integrieren, steht in keiner Beziehung zu dem erwarteten Ergebnis. Java bietet mit dem Java-Card Environment und speziell dem Gateway Modell eine recht gute Möglichkeit, das R&A-Modell zu integrieren. Die Rollen, Aufgaben und restlichen Zustandsvariablen müssen entsprechend auf Java-Klassen abgebildet werden.