Kapitel 7

Sichere elektronische Transaktionen

Die Kommerzialisierung des Internet hat in den letzten Jahren die Frage nach sicheren Verfahren zur Abwicklung von Finanztransaktionen in das Blickfeld öffentlichen Interesses gerückt. Hierzu wurde von uns im Auftrag der Deutschen Bank AG ein Gutachten erstellt, in dem verschiedene Zahlungsprotokolle analysiert werden. Neben diesen Arbeiten haben wir uns insbesondere auch den modernen kryptographischen Verfahren gewidmet. Im Rahmen dieser Untersuchungen konnte auf dem Parsytec GCel–3/1024 des ZPR ein Europarekord für die Faktorisierung großer Zahlen erzielt werden. Für die Firma debis wurde ein Paket zur statistischen Evaluierung kryptographischer Hashfunktionen entwickelt.

7.1 Effiziente Handhabung von Zahlungen mit Kleinstbeträgen im Internet

Wurde bisher das Internet von Unternehmen vornehmlich als Präsentations- und Werbemedium genutzt, rückt heute der elektronische Marktplatz immer mehr in den Vordergrund. Eine notwendige Bedingung für dessen Erfolg ist allerdings die Bereitstellung von geeigneten Zahlungsmöglichkeiten. Mit der Einigung auf ein gemeinsames Protokoll (Secure Electronic Transaction, SET) haben Mastercard und Visa die Voraussetzung für eine standardisierte, einfache und sichere Kreditkartenzahlung im Internet geschaffen.

Neben dem Bestellen und Bezahlen physischer Güter im Internet wird vor allem dem Handel mit Informationen ein großes Wachstumspotential prognostiziert. Für Informationen (z. B. Suchabfragen, Zeitungsartikel) können allerdings nur Kleinstbeträge, die bis zu 10 US-Dollar reichen, erhoben werden. Um eine solche Transaktion dennoch kostengünstig durchführen zu können, sind neuartige Zahlungssysteme zu entwickeln.

In dem Forschungsprojekt sind speziell die Sicherheitsaspekte aus Sicht der Benutzer untersucht worden. Das MilliCent-Protokoll wurde ausgewählt, weil es die Anforderungen an Zahlungen mit Kleinstbeträgen, wie z. B. einen möglichst geringen Kommunikationsaufwand, am besten erfüllte.

Dieses Zahlungsprotokoll ist von uns für weitere detaillierte Analysen prototypisch umgesetzt worden. Für die Benutzer wurde eine spezielle Software (Java-Applet) entwickelt, die über den WWW-Server des ZPR geladen werden kann und auf dem eigenen Computer ausgeführt wird. Auf den Rechnern des ZPR laufen die Server-Programme, die Händler und Bank simulieren. Über die Software des Benutzers können Suchabfragen an eine Suchmaschine („search engine") im ZPR übermittelt werden. Die Suchmaschine hat in ihrem Bestand sämtliche Veröffentlichungslisten und technischen Reports der nordrhein-westfälischen Universitäten (insgesamt 200 Internet-Server). Sie sieht ebenfalls eine Volltext-Suche innerhalb der Arbeiten vor.

Damit haben wir die technischen Voraussetzungen für einen Kauf von Informationen via Internet bereitgestellt. Für die Durchführung einer Suchabfrage und den Erhalt der gewünschten Informationen muß der Benutzer mit digitalem Geld zahlen. Die dafür notwendigen digitalen Münzen werden vom Bank-Server ausgegeben. Als Gegenleistung dafür wurde im Experiment kein *reales* Geld gefordert. Statt dessen mußte der Benutzer einen Fragebogen zur Akzeptanz von Zahlungssystemen für den Kauf von Informationen im Internet ausfüllen. Außerdem sollte herausgefunden werden, welches Maß an Sicherheit für Zahlungen von Kleinstbeträgen notwendig ist. Es wurden vor allem Antworten auf die folgenden Fragen gesucht: Sollen die Sicherheitsanforderungen für Kleinstbeträge ähnlich hoch sein wie bei Zahlungen mit Kreditkarte? Ist man auch bereit, für mehr Sicherheit mehr zu zahlen oder längere Antwortzeiten in Kauf zu nehmen?

Abbildung 7.1 zeigt, wieviele und welche Daten über das Netz ausgetauscht werden müssen, bis der Benutzer die gewünschten Informationen vom Händler gegen virtuelles Geld kaufen kann.

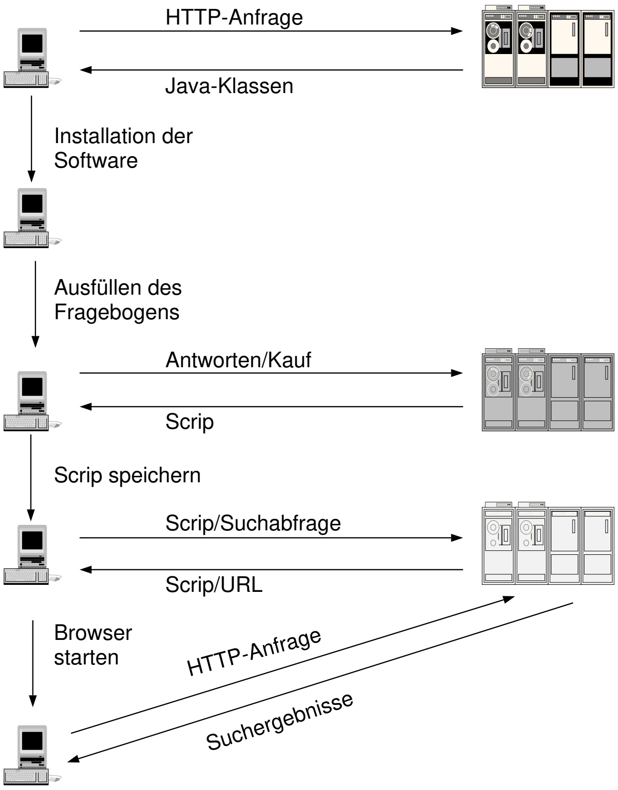

Abbildung 7.1: Ablauf des Experimentes

Die Studie ergab, daß die Benutzer nicht bereit sind, bei Kleinstbeträgen Sicherheitseinbußen hinzunehmen. Digitale Münzen sollen genauso sicher aufbewahrt werden wie kryptographische Schlüssel, die langfristig zum Signieren von Kreditkartenzahlungen eingesetzt werden. Digitale Münzen dürfen bei einer Transaktion nur verschlüsselt übermittelt werden. Für Sicherheitsmaßnahmen nehmen die Benutzer Zeitverzögerungen in Kauf. Höhere Kosten werden allerdings nicht akzeptiert.

7.2 Virtuelle Börse im Internet

Das rasante Wachstum des Internet hat auch für Veränderungen in der Finanz- und Bankenwelt gesorgt. Zahlreiche Banken und Finanzdienstleister sind bereits im Internet mit einem WWW-Server vertreten. Über das Internet werden Dienstleistungen wie Konto- und Depotführung angeboten. Für das ZPR als Forschungseinrichtung ergeben sich aus dieser neuen Technologie eine Reihe von Fragestellungen: Wie können Aufträge sicher über das Internet übermittelt werden? Eignet sich das Internet nur für die Übermittlung von Aufträgen, oder können auch Güter gehandelt werden? Ist ein Wertpapierhandel möglich? Welche Art der Börse empfiehlt sich dabei? Traditionell wird zwischen Auktionärsbörsen, bei denen die Kursbildung durch Makler vorgenommen wird, und Market-Maker-Börsen unterschieden, bei denen sogenannte Market-Maker sich verpflichten, verbindliche Ankaufs- und Verkaufskurse zu veröffentlichen.

Als erster Schritt in diesem Bereich ist vom ZPR eine virtuelle Börse nach dem Auktionärsprinzip konzipiert und realisiert worden. Durch sie konnte einerseits die sichere Auftragsübermittlung sowie die Praktikabilität einer Börse im Internet evaluiert werden. Zukünftig ist geplant, eine Market-Maker-Börse, die neuartige Multicast Backbone (MBONE) Technologien einsetzt, zu realisieren. Konzepte sind bereits auf der SOR-Tagung ’96 einem Fachpublikum vorgestellt worden.

Um für hinreichende Beteiligung an der Testbörse zu sorgen, wurde sie begleitend zur Fußball-Europameisterschaft 1996 in England als virtuelle EM-Börse im Internet organisiert. Es gab eine interne Börse für Mitarbeiter und eine offene Börse, an der sich jeder beteiligen konnte. Insgesamt haben sich rund 90 Personen an den Spielen beteiligt und für einen regen Handel gesorgt.

Bei der Anmeldung zum Spiel erhielt jeder Teilnehmer eine Benutzerkennung und ein Paßwort. Zusätzlich wurde für jeden Teilnehmer ein Konto mit Spielgeld und Mannschaftsanteilen eingerichtet. Der Kauf und Verkauf von Anteilen sowie die Verwaltung der Bestände wurden über das World Wide Web (WWW) mit einem Java-Applet durchgeführt. Informationen zum Spiel können über die beiden URLs

`http://www.zpr.uni-koeln.de/EMBoerse/`

und

`http://www.zpr.uni-koeln.de/ZPRBoerse/`

abgerufen werden.

Die Spieler verfügten über ihr Konto, indem sie Aufträge zum Kauf oder Verkauf von Mannschaftsanteilen an den Server übermittelten. Jede Transaktion mußte zuvor durch Benutzerkennung und Paßwort authentisiert werden. Die Kursermittlung fand zu festgelegten Zeiten statt. Die resultierenden Kurse und Umsätze wurden über das WWW publiziert und graphisch dargestellt.

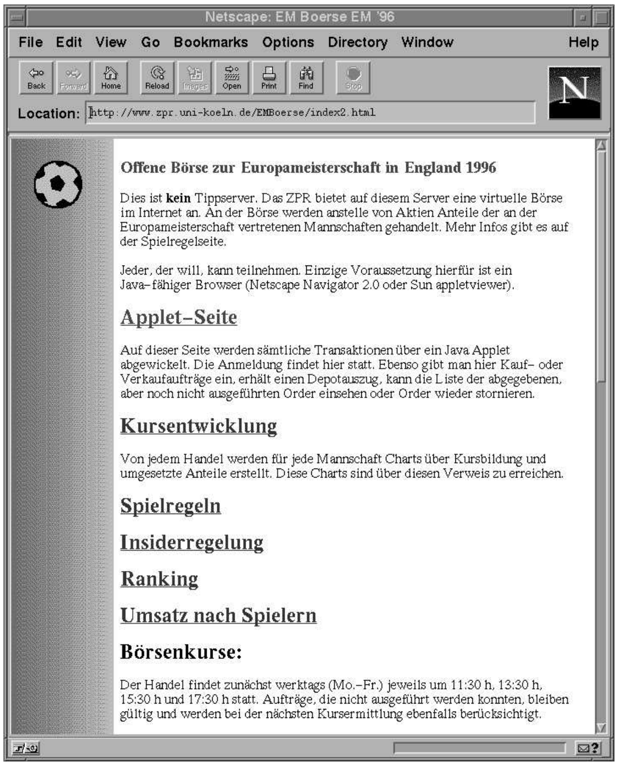

Abbildung 7.2: HTML-Startseite der EM-Börse

Die Funktionalität, die für das Fußball-Börsenspiel benötigt wurde, stimmt im wesentlichen mit den Anforderungen an das Homebanking überein. Authentisierung und Transaktionen müssen in beiden Fällen sicher und einfach zugleich über das Internet durchgeführt werden können. Die Fußballbörse kann daher als Testfeld für Homebanking-Transaktionen betrachtet werden.

Das Börsenspiel hat unter den Teilnehmern reges Interesse hervorgerufen. Viele wünschten sich eine Fortsetzung des Spiels mit der nächsten Fußball-Bundesligasaison. Die Anmeldung der Spieler, Eingabe von Aufträgen und Kursermittlung verlief reibungslos.

7.3 Kryptographie

Neue Parallele Faktorisierungsalgorithmen

Das RSA-Verfahren ist eines der international gebräuchlichsten Verfahren für digitale Signaturen und Verschlüsselungen. Es wird u.a. beim Homebanking (z. B. Bank24), im Internet (z. B. Netscape) und für sichere elektronische Post (z. B. PGP) eingesetzt. Dabei wird ein öffentlicher (d. h. allgemein zugänglicher) und ein privater (d. h. geheimer) Schlüssel verwendet. Mit dem einen Schlüssel wird die Nachricht codiert und mit dem anderen decodiert. Beide Schlüssel müssen für einen Nachrichtenaustausch eingesetzt werden. Der öffentliche Schlüssel ist das Produkt zweier großer Primzahlen.

Die einzige bisher bekannte Methode, das RSA-Verfahren zu brechen, ist die Faktorisierung des RSA-Modulus, d. h. die Berechnung der Primfaktoren des öffentlichen Schlüssels. Die Vorhersage der für die Faktorisierung von Schlüsseln üblicher Größe (384 Bit, 448 Bit, 512 Bit, 576 Bit, usw.) benötigten Rechenzeit ist daher die einzige Möglichkeit, die Sicherheit in der Praxis benutzter RSA-Systeme zu beurteilen.

Während die Probedivision schon bei Zahlen von 20 Dezimalstellen (ca. 70 Bit) an ihre Grenze stößt, können mit neuen Algorithmen (Quadratisches Sieb 1986, Zahlkörpersieb 1993) Zahlen mit mehr als 100 Dezimalstellen zerlegt werden. Beide Verfahren haben asymptotisch eine subexponentielle Laufzeit. Die theoretischen Analysen geben jedoch wenig Auskunft über die tatsächlich benötigte Rechenzeit für reale Instanzen. Zuverlässige Extrapolationen von erfolgreich zerlegten Zahlen sind nur über ca. zehn weitere Dezimalstellen möglich.

Das quadratische Sieb und das Zahlkörpersieb enthalten eine Siebphase und die Lösung eines Gleichungssystems über GF(2), das Zahlkörpersieb darüber hinaus die Bestimmung einer Quadratwurzel in einem Zahlkörper. Die Siebphase ist mit mehreren Jahren Rechenzeit auf einer Workstation bei einem 384-Bit-Modulus der bei weitem zeitaufwendigste Teilschritt und wurde auf einer Vielzahl von Parallelrechnern implementiert (Workstation-Cluster, Parsytec GCel, PowerXplorer, IBM SP1, usw.). Den Engpaß der Siebphase bilden Speicherarchitektur und Speicherverwaltung der jeweiligen Maschine. Hier haben wir für RISC-Maschinen eine schnelle Umsetzung entwickelt. U. a. gelang uns die Faktorisierung einer 116-stelligen Zahl aus dem Cunningham-Projekt – ein Europarekord (siehe Abb. 7.3).

Lineare Gleichungssysteme über GF(2)

Die zu lösenden 0-1-Gleichungssysteme der Faktorisierungsalgorithmen aus dem letzten Abschnitt beinhalten Matrizen mit mehreren hunderttausend Zeilen und Spalten. Die auftretenden Matrizen sind sehr dünn besetzt (weniger als 0,1% Nichtnulleinträge), im Gegensatz zu ähnlichen Problemen aus der Numerik jedoch unstrukturiert.

1887862087 5723998168 9743641888 6918839936 7217878748 2480424977
1415241615 5049698272 1057735455 4056878380 0947100792 480453

=

3322172551 3143762321 3856700096 1500096409 0592582538 8563831805 3320936174 4317449755 33

×

5682612984 1614959843 5231149526 9241

Abbildung 7.3: *Faktorisierung einer 116-stelligen Zahl*

Gewöhnliche Gauß-Elimination ist wegen der entstehenden Zeit- und Platzprobleme indiskutabel.

Die jüngste Entwicklung stellt das Block-Lanczos-Verfahren von P. L. Montgomery für GF(2) dar, das explizit die Wortgröße der benutzten Maschine (32 Bit, 64 Bit) einbezieht. Hier haben wir eine Shared-Memory Parallelisierung auf der SGI Power Challenge-Maschine des Rechenzentrums begonnen. Erste parallele Ergebnisse konnten bereits nach nur einer Woche erzielt werden, da – im Gegensatz zu einer Distributed Memory Parallelisierung – nur zeitkritische Teile parallelisiert werden müssen. Auf acht Prozessoren haben wir einen (vorläufigen) Speedup von 4,8 erzielt.

Statistische Untersuchungen kryptographischer Hashfunktionen

Mit kryptographischen Hashfunktionen können „Fingerabdrücke“ elektronischer Dokumente effizient berechnet werden. Der Fingerabdruck wird dann zeitaufwendiger verschlüsselt und dient als elektronische Unterschrift des jeweiligen Dokumentes. Gute kryptographische Hashfunktionen müssen sicher sein: So darf es z.B. keine praktische Möglichkeit geben, zwei verschiedene Nachrichten mit demselben Fingerabdruck zu konstruieren. Notwendigerweise müssen kryptographische Hashfunktionen dazu eine Reihe von statistischen Tests passieren.

Ein in Kooperation mit der debis Systemhaus GmbH, Bonn, entwickeltes Programmpaket für statistische Tests kryptographischer Hashfunktionen wurde im Januar 1995 erfolgreich abgenommen. Neben klassischen Standardverfahren lagen hier die Schwerpunkte bei algebraischen Zykeltests und der effizienten Suche nach Linear- und Pseudolinearfaktoren.

Mit den implementierten Zykeltests können für eine Funktion mit identischem Definitions- und Wertebereich Eigenschaften wie Abgeschlossenheit, Injektivität und Fixpunktfreiheit entschieden werden. Darüber hinaus kann beurteilt werden, ob das von der Größe der Schlüsselmenge suggerierte Sicherheitsmaß realistisch ist oder nicht.

Ziel der in der Literatur zuvor nur wenig dokumentierten Linear- und Pseudolinearfaktortests ist die Suche nach (pseudo-)linearen Abhängigkeiten innerhalb der Ausgabestellen bei gleichzeitiger Änderung einer bestimmten Menge von Eingabestellen. Dazu wurden neue Verfahren zur Bestimmung von Linear- und Pseudolinearfaktoren entwickelt und implementiert, die u. a. alle Pseudolinearfaktoren mit einer Wahrscheinlichkeit oberhalb einer vorgegebenen Schranke bestimmen.

Zu einer vollständigen Beurteilung der Qualität der kryptographischen Hashfunktion müssen die Ergebnisse im allgemeinen um eine manuelle Analyse der Funktion erweitert werden.