Digitale Signaturen für Datenströme

Vom Fachbereich
Elektrotechnik und Informatik der Universität Siegen
genehmigte Dissertation
zur Erlangung des akademischen Grades

Doktor der Ingenieurwissenschaften
(Dr.-Ing.)

von Dipl.-Ing. Niko Schweitzer

Referent:	Prof. Dr. rer. nat. Christoph Ruland
Korreferent:	Prof. Dr.-Ing. Firoz Kaderali
Tag der Einreichung:	7. November 2002
Tag der mündlichen Prüfung:	18. März 2003

UNIVERSITÄT SIEGEN

Schriften zur Nachrichtenübermittlungstechnik

Herausgeber: Prof. Dr. Christoph Ruland

Band 7

Niko Schweitzer

Digitale Signaturen für Datenströme

Aachen 2003

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Schweitzer, Niko:
Digitale Signaturen für Datenströme / Niko Schweitzer.
Aachen : Shaker, 2003
(Schriften zur Nachrichtenübermittlungstechnik ; Bd. 7)
Zugl.: Siegen, Univ., Diss., 2003
ISBN 3-8322-1417-8

Printed in Germany.

ISBN 3-8322-1417-8
ISSN 1431-6560

Shaker Verlag GmbH • Postfach 101818 • 52018 Aachen
Telefon: 02407 / 95 96 - 0 • Telefax: 02407 / 95 96 - 9
Internet: www.shaker.de • eMail: info@shaker.de

Vorwort

Die vorliegende Arbeit entstand während meiner Tätigkeit als Wissenschaftlicher Mitarbeiter am Institut für Nachrichtenübermittlung der Universität Siegen.

Dem Institutsleiter, Herrn Prof. Dr. rer. nat. Christoph Ruland, danke ich herzlich für die Möglichkeit zur Durchführung dieser Arbeit, die eingeräumte eigenverantwortliche Arbeitsweise und die ständige Bereitschaft zur wissenschaftlichen Diskussion sowie für seine wertvollen Hinweise und Anregungen.

Mein Dank gilt ferner Herrn Prof. Dr.-Ing. Firoz Kaderali, Leiter des Lehrstuhls Kommunikationssysteme der Fernuniversität Hagen, für sein Interesse an dieser Arbeit und die Übernahme des Korreferates.

Auch möchte ich mich bei Herrn Prof. Dr. Wolfgang Merzenich für den Vorsitz der Prüfungskommission bedanken.

Weiterhin danke ich meinen Kollegen Christian Geuer-Pollmann, Christine Haßler, Luigi Lo Iacono, Oliver Jung, Sven Kuhn, Matthias Schneider, Christoph Stepping und Kai Wollenweber für die stets konstruktive Zusammenarbeit und die ausgesprochen angenehme Arbeitsatmosphäre.

Besonderer Dank gilt Katja Bertolo und allen meinen Freunden, die mich stets beim Verfassen dieser Arbeit motiviert und auch manchmal auf andere Gedanken gebracht haben.

Meinen Eltern danke ich dafür, dass sie mir das Studium ermöglichten, mich stets unterstützt und gefördert haben.

Siegen, im Januar 2003

Niko Schweitzer

Zusammenfassung

Durch die Verbreitung und Entwicklung vernetzter Rechnersysteme wie das Internet entstehen vielfältige Sicherheitsprobleme. Berichte über Angriffe und Schäden durch Computerviren, Trojanische Pferde oder Hacker verdeutlichen den Bedarf nach geeigneten Schutzmaßnahmen. Zusätzliche Sicherheitsanforderungen entstehen durch Bestrebungen, elektronische Geschäftsprozesse, häufig als E- oder M-Commerce bezeichnet, über offene Netzwerke wie das Internet abzuwickeln. Neben dem bekanntesten Schutzziel, Kommunikationsinhalte oder Kommunikationsbeziehungen vertraulich zu halten, werden Sicherheitsdienste wie Prüfbarkeit der Authentizität digitaler Daten zunehmend bedeutender.

Zur Gewährleistung der Authentizität sind digitale Signaturen ein anerkannter und vielfältig nutzbarer kryptographischer Mechanismus. Signaturalgorithmen besitzen allerdings den Nachteil, Berechnungen erst durchführen zu können, wenn vollständige Datensätze verfügbar sind. Ist eine zeitnahe Be- oder Verarbeitung von Daten erforderlich, sind diese meist ungeeignet und nicht anwendbar.

Gefördert durch steigende Bandbreite digitaler Netzwerke entstehen vermehrt Anwendungen, die Datenströme übertragen und zeitnah verarbeiten. Gängige Beispiele sind digitale Audio-, Video- oder Datenübertragungen, die direkt während des Empfangs konsumiert werden, ohne eine vollständige Speicherung von Datensätzen vorzunehmen. Um in solchen Anwendungsbereichen auf digitalen Signaturen basierende Sicherheitsdienste anbieten zu können, ist die Entwicklung und Untersuchung spezieller Algorithmen und Verfahren erforderlich.

Die vorliegende Arbeit behandelt die Problematik der Berechnung und Verifikation digitale Signaturen für Datenströme. Es werden Authentikationsverfahren für Datenströme vorgestellt sowie neue Datenstrom-Signaturverfahren entwickelt, beschrieben und untersucht.

Der praktische Teil der Arbeit beschreibt ein entwickeltes Framework zur Implementation und Nutzung von Datenstrom-Signaturverfahren in Java. Weiterhin werden Implementationen und Messergebnisse dargestellt.

Abstract

With the rapid growth of open communication networks like the Internet more and more incident reports of damages caused by computer viruses, malicious software or hacker attacks are published. This obviously illustrates the demand for security services to prevent and detect attacks. Additional security requirements arise from electronic business transactions performed over insecure networks. Besides the objective of keeping communications confidential other security services as data integrity and authenticity become increasingly important.

Digital signatures are a frequently used cryptographic primitive to ensure authenticity of digital data. Signing digital streams is however more problematic as signing messages in whole. Traditional signature schemes are message oriented and require entire datasets for signature calculation and verification.

Digital streams are very long (or potentially infinite) sequences of bits which are sent to one or multiple receivers and are processed and consumed more or less at input rate without much delay. Therefore it is infeasible to obtain and store streams entirely in order to check authenticity by applying traditional digital signature schemes. Streams may include for instance online news, stock and data feeds, radar and medical data transmissions or digitized audio and video.

This work focuses on signing digital streams. After describing difficulties arising from streamed data processing, requirements for stream signatures are discussed and interesting application areas are pointed out. In the main part various new signature schemes for signing streamed data are presented and system properties are worked out.

The practical part introduces a flexible framework for implementation and usage of stream signature schemes in Java. Furthermore implementation results are presented.

Inhaltsverzeichnis