

Erik-Oliver Blaß

Analyse, Verifikation und Realisierung
kryptographischer Protokolle fuer flexible
Zugriffe auf medizinische Datenbanken

Diplomarbeit

BEI GRIN MACHT SICH IHR WISSEN BEZAHLT



- Wir veröffentlichen Ihre Hausarbeit, Bachelor- und Masterarbeit
- Ihr eigenes eBook und Buch - weltweit in allen wichtigen Shops
- Verdienen Sie an jedem Verkauf

Jetzt bei www.GRIN.com hochladen
und kostenlos publizieren



Bibliografische Information der Deutschen Nationalbibliothek:

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de/> abrufbar.

Dieses Werk sowie alle darin enthaltenen einzelnen Beiträge und Abbildungen sind urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsschutz zugelassen ist, bedarf der vorherigen Zustimmung des Verlanges. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen, Auswertungen durch Datenbanken und für die Einspeicherung und Verarbeitung in elektronische Systeme. Alle Rechte, auch die des auszugsweisen Nachdrucks, der fotomechanischen Wiedergabe (einschließlich Mikrokopie) sowie der Auswertung durch Datenbanken oder ähnliche Einrichtungen, vorbehalten.

Impressum:

Copyright © 2001 GRIN Verlag
ISBN: 9783638130981

Dieses Buch bei GRIN:

<https://www.grin.com/document/5101>

Erik-Oliver Blaß

Analyse, Verifikation und Realisierung kryptographischer Protokolle fuer flexible Zugriffe auf medizinische Datenbanken

GRIN - Your knowledge has value

Der GRIN Verlag publiziert seit 1998 wissenschaftliche Arbeiten von Studenten, Hochschullehrern und anderen Akademikern als eBook und gedrucktes Buch. Die Verlagswebsite www.grin.com ist die ideale Plattform zur Veröffentlichung von Hausarbeiten, Abschlussarbeiten, wissenschaftlichen Aufsätzen, Dissertationen und Fachbüchern.

Besuchen Sie uns im Internet:

<http://www.grin.com/>

<http://www.facebook.com/grincom>

http://www.twitter.com/grin_com

Diplomarbeit

Analyse, Verifikation und Realisierung kryptographischer Protokolle für flexible Zugriffe auf medizinische Datenbanken



Universität Karlsruhe
Fakultät für Informatik
Institut für Algorithmen
und Kognitive Systeme

Erik-Oliver Blaß

Betreuer: Prof. Dr. Thomas Beth
Betreuender Mitarbeiter: Dipl. Inform. Jörg Moldenhauer

8. Oktober 2001

Erklärung

Ich versichere, diese Arbeit selbständig verfaßt und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt zu haben.

Karlsruhe, den 8. Oktober 2001

(Erik-Oliver Blaß)

Kurzfassung

Der Umgang mit sensiblen Patientendaten stellt hohe Anforderungen an deren Vertraulichkeit und Integrität. Für einen entfernten, elektronischen Zugriff auf solche Daten und deren elektronische Verarbeitung sind besondere Sicherheitsvorkehrungen nötig, um Geheimhaltung und Schutz vor Mißbrauch zu gewährleisten. Ein Problem dabei sind insbesondere die zeitlich veränderlichen Zuständigkeiten und Verantwortlichkeiten für Patientendaten im klinischen Alltag.

In dieser Arbeit werden auf bestehenden kryptographischen Komponenten basierende Protokolle zum Zugriff auf medizinische Daten entwickelt, die diese Anforderungen gezielt umsetzen. Dazu gehören die gesicherte Speicherung der medizinischen Daten in speziell hierfür entwickelten Datenbanken sowie eine funktions-spezifische Rechtverwaltung und Zugangskontrolle mittels sogenannter Rollen.

Die erarbeiteten Protokolle und das Umfeld ihres Einsatzes werden auf verschiedenen Ebenen analysiert und ihre Sicherheit formal bewiesen. Mit einer Implementierung in Java wird die Einsatzfähigkeit der Protokolle gezeigt. Die Verwendung von CORBA-Kommunikationsmechanismen erlaubt die Einbindung in ein verteiltes medizinisches Informationssystem, das vom IAKS im Rahmen des Teilprojekts Q6 des SFB 414 „Informationstechnik in der Medizin“ als Prototyp entwickelt wird.

Inhaltsverzeichnis

| | | |
|----------|---|-----------|
| 1 | Einleitung | 1 |
| 1.1 | Aufgabenstellung | 2 |
| 1.2 | Sicherheitsrelevante Anforderungen | 4 |
| 2 | Kryptographie | 7 |
| 2.1 | Chiffren | 7 |
| 2.1.1 | AES | 8 |
| 2.1.2 | RSA | 9 |
| 2.2 | Digitale Signaturen | 10 |
| 2.2.1 | SHA-1 | 11 |
| 2.2.2 | Zertifikate und Zertifizierungsstellen | 12 |
| 2.3 | Shared-Secrets | 13 |
| 2.4 | Kommutative Chiffren | 15 |
| 2.4.1 | One-Time-Pad | 15 |
| 2.4.2 | Drei-Wege-XOR | 16 |
| 2.5 | Zufallszahlen | 16 |
| 2.6 | Logic of Authentication | 19 |
| 2.6.1 | Notation der Logic of Authentication | 20 |
| 2.6.2 | RVLogik, eine Erweiterung der BAN-Logik | 24 |
| 3 | Protokolle | 29 |
| 3.1 | Gemeinsamkeiten der entwickelten Protokolle | 29 |
| 3.2 | Shared Protokoll | 30 |
| 3.2.1 | Zertifikate | 32 |
| 3.2.2 | Formalisierte Nachrichten | 33 |

| | | |
|----------|---|-----------|
| 3.3 | Zyklisches Protokoll | 41 |
| 3.3.1 | Ablauf | 42 |
| 3.3.2 | Formalisierte Nachrichten | 44 |
| 3.4 | Geschwindigkeit und Bewertung | 49 |
| 3.5 | Update-Mechanismus | 51 |
| 4 | Analyse | 53 |
| 4.1 | Verwendete Chiffren | 54 |
| 4.1.1 | AES, RSA und SHA-1 | 54 |
| 4.1.2 | Shared-Secrets | 56 |
| 4.1.3 | FIPS 140-1 | 56 |
| 4.1.4 | Bewertung | 57 |
| 4.2 | Logic of Authentication | 58 |
| 4.2.1 | Grundlagen | 58 |
| 4.2.2 | Erforderliche Anpassungen | 58 |
| 4.2.3 | Shared Protokoll | 59 |
| 4.2.4 | Zyklisches Protokoll | 63 |
| 4.3 | Laufzeitumgebung | 67 |
| 4.3.1 | Vom Quell-Code zur JVM | 67 |
| 4.3.2 | Risiken und Schutzmechanismen der JVM | 67 |
| 4.3.3 | CORBA | 70 |
| 4.4 | Implementierung | 71 |
| 4.5 | Denial of Service | 73 |
| 4.5.1 | Verbrauch begrenzter Ressourcen | 73 |
| 4.5.2 | Verändern der Konfiguration | 74 |
| 4.5.3 | Physikalische Zerstörung | 75 |
| 5 | Implementierung | 77 |
| 5.1 | iSaSilk | 77 |
| 5.2 | Shared-Secrets | 78 |
| 5.3 | Generieren von Zufallszahlen | 79 |
| 5.4 | ProcessQueryWrapper | 81 |
| 5.5 | Rollenproxy | 82 |

| | | |
|----------|---|-----------|
| 5.5.1 | Crypt | 83 |
| 5.5.2 | Rollenverwaltung | 83 |
| 5.5.3 | Durchführung der Protokolle | 84 |
| 5.5.4 | Sicherheit der RoleProxy-Klasse | 85 |
| 5.6 | Update-Mechanismus | 86 |
| 5.7 | Benutzen der Protokolle | 87 |
| 5.8 | CORBA | 88 |
| 5.9 | Änderungen am RVChecker | 89 |
| 5.10 | Werkzeuge | 90 |
| 5.10.1 | Annotationen | 90 |
| 5.10.2 | Pseudonymisierer | 95 |
| 6 | Zusammenfassung | 99 |