Distributionskontrolle von Dokumenten

Ulrich Pinsdorf[1] · Roland Krüger[2] · Ursula Oesing[2]

[1]Fraunhofer Institut für Graphische Datenverarbeitung
ulrich.pinsdorf@igd.fraunhofer.de

[2]MediaSec Technologies AG
{rkrueger|uoesing}@mediasec.de

Zusammenfassung

Information ist für die meisten Unternehmen eine erfolgskritische Ressource. Die absichtliche oder versehentliche Veröffentlichung vertraulicher Dokumente ist i.d.R. mit einem Schaden für das Unternehmen verbunden. Sicherheitspolitiken beschreiben zwar abstrakt, was mit einem Dokument geschehen darf und wo es gespeichert werden kann. Doch das zeitnahe Erkennen von Konflikten und die Durchsetzung der Sicherheitsregeln ist oft ein Problem. In diesem Artikel wird ein Softwaresystem beschrieben, das die Einhaltung von Sicherheitspolitiken für Dokumente gewährleistet. Die beiden Kerntechnologien, die dabei zum Einsatz kommen, sind elektronische Wasserzeichen und mobile Agenten. Die Klassifikation eines Dokumentes gemäß der unternehmensweiten Sicherheitspolitik wird mittels elektronischer Wasserzeichen in das Dokument selbst eingebracht. Zudem wird allen Speicherorten eine Sicherheitsstufe zugeordnet, die festlegt, welche Dokumentklassen dort abgelegt werden dürfen. Um die im Unternehmensnetz vorhandenen Rechner und Datenspeicher effizient und umfassend zu durchsuchen, werden mobile Agenten eingesetzt. Diese Programme migrieren periodisch auf alle Rechner und nehmen eine Untersuchung vor. Bei Verstößen gegen die Sicherheitspolitik können Agenten definierte Maßnahmen ergreifen, um Schaden vom Unternehmen abzuwenden.

1 Motivation

Die Ressource *Information* bekommt als kritischer Erfolgsfaktor von Unternehmen eine immer höhere Bedeutung. Die Gründe hierfür sind vielfältig, etwa der Bedarf zum zeitnahen Informationsaustausch mit Kunden, Lieferanten oder mit entfernten Unternehmensstandorten. Darüber hinaus werden auch innerhalb der Unternehmen die Arbeitsabläufe durch elektronische Medien unterstützt oder sogar komplett durch diese abgebildet. Der Informationsaustausch mittels E-Mail, elektronischen Antragsverfahren oder elektronischen Dokumentenverwaltungs- und Workflow-Managementsystemen gewinnt eine immer höhere Bedeutung. Durch die effiziente Verwaltung und Weiterleitung von Information mit elektronischen Medien lassen sich Arbeitsabläufe optimieren, Durchlaufzeiten reduzieren und interne Ressourcen einsparen.

Durch den umfangreichen Gebrauch der unternehmenskritischen Ressource Information steigen auch die Anforderungen an die Informationssicherheit in Unternehmen. Die Gewährleitung reibungsloser Abläufe erfordert dementsprechend effektivere Schutzmechanismen. Zusätzlich nehmen datenschutz- und informationsrechtliche Fragestellungen eine immer wichti-

P. Horster (Hrsg.) · Elektronische Geschäftsprozesse 2004 · syssec (2004) 485-499.

gere Stellung im Bereich der Rechtssprechung ein, so dass die Informationssicherheit auch diesen Bereich abdecken muss.

Die Überwachung elektronischer Dokumentenflüsse stellt Unternehmen vor große Probleme. Das versehentliche oder gar beabsichtigte Weitergeben vertraulicher Dokumente auf elektronischem Weg erfordert keinen Aufwand, kann aber empfindlichen Schaden anrichten. Darum ist es wünschenswert die Distribution von Dokumenten automatisch zu überwachen, um ggf. eingreifen zu können, bevor sensible Daten einen geschützten Bereich verlassen.

Im Rahmen dieses Artikels wird eine automatische Methode vorgestellt, um Dokumentenflüsse mittels elektronischer Wasserzeichen und mobiler Softwareagenten zu überwachen. Grundidee ist, dass die mobilen Agenten eingesetzt werden um Sicherheitsvorfälle in Unternehmensnetzwerken zu erkennen und geeignet zu reagieren. Die Erkennung solcher Sicherheitsvorfälle basiert auf einer Kombination der Kennzeichnung von Dokumenten mit digitalen Wasserzeichen und dem Abgleich der Wasserzeicheninformation mit definierten Sicherheitspolitiken.

Im Folgenden werden verwandte Arbeiten zum vorliegenden Ansatz angeführt. Danach stellt Abschnitt 3 die beiden involvierten Technologien kurz vor. In Abschnitt 4 wird die Problemstellung definiert. Unser Lösungsansatz wird in den Abschnitten 5 und 6 beschrieben. Abschließend fasst Abschnitt 7 den Artikel zusammen und nimmt eine erste Bewertung vor.

2 Verwandte Arbeiten

Es gibt im Umfeld mobiler Agenten eine Reihe von Arbeiten, die das Durchsuchen lokaler Datenbestände mit mobilem Code vorschlagen. Roth verwendet mobile Agenten um Bilddatenbanken effizient mit Ähnlichkeitsalgorithmen für Bilder zu durchsuchen [Roth01]. Das System CARROT II [CKM+01] wurde in einer Projektgruppe um Nicholas und Cost an der Universität Maryland entwickelt und wird zum Dokumenten-Management und Informationsaustausch genutzt. Der Ansatz arbeitet mit kooperierenden stationären Agenten. Interessant an CARROT II ist die Unterstützung verschiedener Information-Retrieval-Werkzeuge für die Agenten, die es erlaubt andere Inhalte als Texte zu untersuchen. Ein Ansatz, der Wasserzeichen und mobile Agenten direkt verbindet, findet sich in Zhao [ZhLu99].

3 Grundlegende Technologien

In diesem Abschnitt wird ein kurzer Überblick über die Kerntechnologien digitale Wasserzeichen und mobile Agenten gegeben, die im Zuge des zu beschreibenden Lösungsansatzes zum Einsatz kommen.

3.1 Digitale Wasserzeichen

Die Grundidee der digitalen Wasserzeichen besteht darin, eine Information so in ein multimediales Dokument (z.B. Bild, Video-, Audiosignal, PDF-Datei) zu integrieren, dass die Modifikation des Dokuments für den Menschen nicht wahrnehmbar ist. Das konkrete Verfahren hängt dabei immer von dem unterliegenden Medium ab. Für jedes Medium gibt es eine ganze Reihe von Algorithmen und Verfahren, die je nach Anwendungsgebiet unterschiedlich gut geeignet sind. Einen guten Überblick über aktuelle Verfahren und mathematische Hintergründe findet man in [ArSW03]. Bei Bild-, Video- und Audiomaterial ist bspw. die Verwendung

einer mathematischen Transformation (Fourier- oder verwandte Transformationen) eine häufige Realisierung. Die Information wird dann über Modifikationen im Frequenzbereich eingebettet. Nach der inversen Transformation erscheint die eingebrachte Information als zusätzliches, kaum wahrnehmbares Rauschen in dem Medium. Sie wird mit dem Trägermedium verbunden. Die folgende Abb. 1 zeigt ein Beispiel für ein frequenzraumbasiertes Wasserzeichenverfahren.

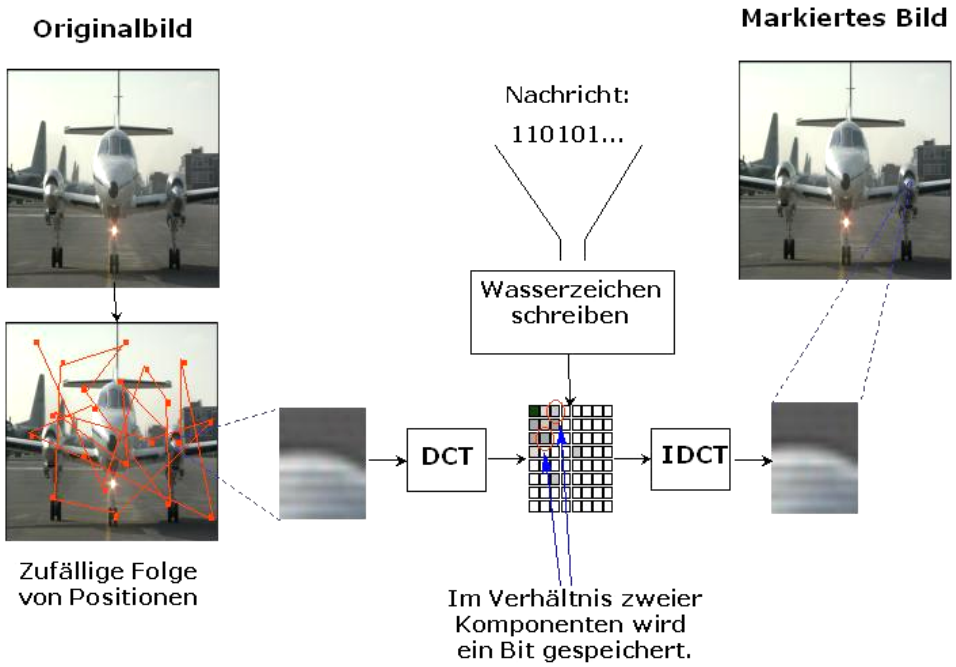

Abb. 1: Schema eines Bildwasserzeichen-Verfahrens am Beispiel des SysCoP®-Algorithmus

Neben der Klassifizierung nach mathematischen Grundlagen, Medientypen oder Dateiformaten können die einzelnen Wasserzeichenverfahren auch nach der Verwendung kryptographischer Verfahren unterschieden werden. Bei einigen Wasserzeichenverfahren erfordert das Auslesen der eingebetteten Information aus einem Dokument die Kenntnis eines geheimen Schlüssels. Abb. 2 zeigt ein Schema für die Verwendung eines Geheimnisses bei der Einbettung von Wasserzeicheninformationen in ein Dokument. Solche Verfahren werden bei speziellen Anwendungen eingesetzt, z.B. zum Nachweis der Urheberschaft.

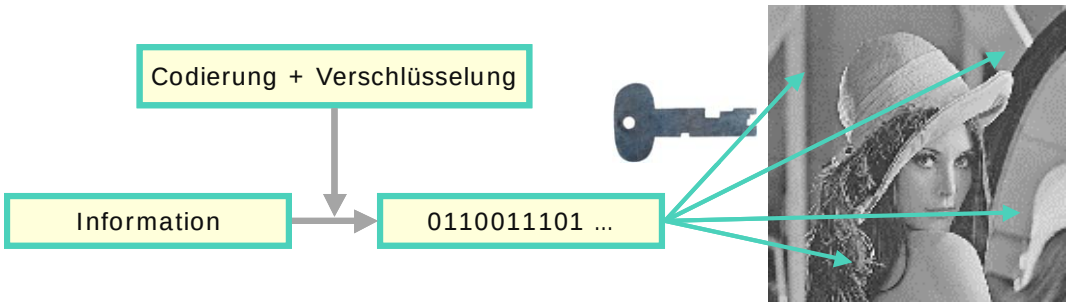

Abb. 2: Verwendung kryptographischer Verfahren bei der Wasserzeicheneinbettung

Zum Nachweis der Urheberschaft als Anwendung digitaler Wasserzeichen wird üblicherweise eine Kennungsinformation über die Person des Urhebers eingebettet. Dieser kann das markierte Dokument automatisiert im Internet suchen und im Fall einer unberechtigten Wieder-

veröffentlichung seine Rechte an dem Material geltend machen. Andere Anwendungen erfordern das Einbringen von Identifikations- oder Zugriffsinformationen in Dokumente.

Abb. 3: Wasserzeichen mit Robustheit 10

Abb. 4: Wasserzeichen mit Robustheit 30

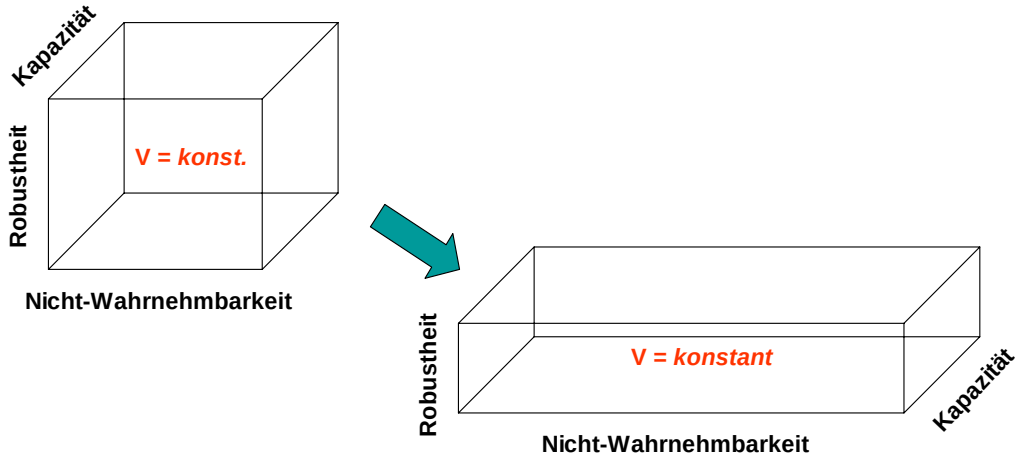

Abb. 5: Abhängigkeit der Parameter Kapazität, Robustheit und nicht Nicht-Wahrnehmbarkeit

Auch die Parametrisierung der Algorithmen ist von großer Bedeutung. Abb. 3 und Abb. 4 zeigen zwei Beispiele eines mit einem Wasserzeichen versehenen Bildes. Bei der Einbettung des Wasserzeichens wurde der Parameter Robustheit variiert. Dies hat deutliche Auswirkungen auf die Wahrnehmbarkeit des Wasserzeichens. Die drei wichtigsten Parameter für Wasserzeichen Robustheit, Nicht-Wahrnehmbarkeit und Kapazität hängen wechselseitig voneinander ab. Abb. 5 verdeutlicht diesen Zusammenhang zwischen den drei wichtigsten Parametern auf anschauliche Weise. Die Parameter Robustheit, Nicht-Wahrnehmbarkeit und Kapazität bilden die drei Raumkoordinaten eines Quaders. Die Erfahrung zeigt, dass das Volumen dieses Quaders bei unterschiedlichen Parametrisierungen in etwa konstant bleibt, d.h. erhöht man einen der Parameterwerte, so ändern sich die beiden anderen entsprechend. Weitergehende Informationen zu digitalen Wasserzeichen behandeln etwa [ArSW03, KoZh95, ZhKo95, BuKZ98].

Diese Abhandlungen betrachten vor allem die Abhängigkeit zwischen Robustheit, Nicht-Wahrnehmbarkeit und Kapazität von Wasserzeichen in der konkreten Anwendung. [CKLS97] geht allgemein auf Verfahren digitaler Wasserzeichen ein, die im Frequenzraum arbeiten.

3.2 Mobile Agenten

Das vom lateinischen Wort *agere* (handeln, wirken) abstammende Wort Agent bezeichnet ursprünglich einen Geschäftsträger im politischen Sinn. Im Kontext der Informatik ist der Begriff des Agenten etwa seit Ende der 70er Jahre bekannt [Brau99]. Die exakte Definition eines Agenten ist in der Fachliteratur nicht eindeutig. Eine sehr verbreitete Herangehensweise an die Definition eines intelligenten Agenten ist die Aufzählung einer Reihe von Fähigkeiten, die einen Agenten von einem Software-Objekt unterscheiden. Eine weit verbreitete solche weiche Definition eines Agenten ist die von Woolridge und Jennings [WoJe95] aufgestellte Definition, die einen Agenten als ein Computer-System mit den Eigenschaften autonom, sozial, reaktiv und proaktiv beschreibt.

Ein weiteres Merkmal von Software-Agenten ist deren Fähigkeit zur Migration; man unterscheidet hier zwischen den Begriffen des stationären Agenten und des mobilen Agenten. Der Begriff des Mobilen Agenten wurde Anfang der 90er Jahre von der Firma General Magic, die seit 1997 ein Patent für diese Technologie hat, geprägt. Die US Patentschrift 5603031 beschreibt mobile Agenten als autonome Programme, die sich in einem heterogenen Netzwerk fortbewegen können und im Auftrag des Benutzers Dienste verrichten [Uspa97]. Ein Agent kann selbst entscheiden, ob und wohin er migrieren möchte.

Der spezielle Unterschied zwischen einem mobilen Agenten und einem herkömmlichen Programm, das von Rechner zu Rechner kopiert und dort immer wieder neu gestartet wird, liegt in dem Umstand, dass die Fortbewegung beim Agenten innerhalb eines Lebenszyklus geschieht. Er wird für den Transport zu einem anderen Rechner nicht gestoppt und auf dem Zielhost *neu* gestartet, sondern nur "eingefroren". Das Programm terminiert dabei nicht, sondern der Kontrollfluss wird unterbrochen und später auf einer anderen Ausführungseinheit wieder aufgenommen. Im Idealfall wird er an genau der Stelle fortgesetzt, an der er unterbrochen wurde. In der Praxis ist es jedoch häufig so, dass der Kontrollfluss des Agenten an einem vereinbarten Punkt neu angesetzt wird [Brau99].

Die Migration erlaubt also das Verschieben eines laufenden Programms auf eine andere Ausführungseinheit. Der Prozesszustand des Programms bleibt dabei erhalten. Dafür wird der aktuelle Programmzustand, also die Menge aller Variablenwerte, die das Programm konstituieren, gespeichert. Diese Eigenschaft heißt Persistenz.

Möchte ein mobiler Agent auf einen entfernten Host migrieren, so teilt er den Migrationswunsch dem lokalen Server mit. Wird diesem Wunsch seitens des Servers stattgegeben, wird der Agent angehalten, der Programmcode und die persistenten Variablen serialisiert und zum Zielrechner transferiert. Dort wird der empfangene Bitstrom wieder deserialisiert und die persistenten Variablen und Datenstrukturen mit den ursprünglichen Werten initialisiert. Das Ergebnis ist ein Abbild des mobilen Agenten vom Speicher des Quellhosts in den Speicher des Zielhostes zum Zeitpunkt der Serialisierung.

Um diese Fähigkeiten zu gewährleisten, müssen alle in dem Netzwerk verbundenen Rechner über eine bestimmte Infrastruktur verfügen, um die Ausführung der Agenten zu ermöglichen. Diese Infrastruktur stellt bspw. alle Mechanismen und Dienste zur Verfügung, die der Agent

zur Ausführung, Migration und Kommunikation benötigt. Eine derartige Infrastruktur wird als Agentenplattform bezeichnet. Um ihre Aufgabe erfüllen zu können, müssen die Agenten mit der Agentenplattform, ggf. auch mit anderen Agenten, kommunizieren können.

Vorteil eines Systems mobiler Agenten ist u.a. die, verglichen mit dem Client-Server-Modell, starke Reduktion der Netzwerkbelastung [LaOs99]. Außerdem ermöglicht dieses Konzept, unterschiedliche Aufgaben an mobile Agenten zu verteilen und sie eigenständig und unabhängig vom sendenden Programm bearbeiten zu lassen [PiBu03]. Ein weiterer Vorteil ist die Entkopplung des Anbietens und der Verwendung von Daten. Da der Absender des Agenten, also der Anfrager einer Datenquelle, den Programmcode des Agenten bestimmt, wird der Agent mit einem Anfrager-spezifischen Programm auf den angebotenen Daten operieren. So kann auf ein und derselben Datenquelle von unterschiedlichen Agenten mit unterschiedlichen Algorithmen gearbeitet werden. In klassischen Client-Server-Systemen gibt der Datenanbieter auch den Verarbeitungsalgorithmus vor. Andererseits bringt der Ansatz der mobilen Agenten neue Sicherheitsrisiken mit sich. Zum einen können bösartige Agenten eine Gefahr darstellen für das Rechnernetz, die Agentenplattform und andere Agenten. Zum anderen sind die gutartigen Agenten potentiell selbst bedroht durch eine manipulierte, böswillige Agentenplattform. Ein konkretes System mobiler Agenten muss diese Bedrohungsszenarien in Betracht ziehen und ihnen durch geeignete Sicherheitsmaßnahmen begegnen.

4 Problemstellung

Konkrete Anforderungen an die Dokumenten- und Informationssicherheit in Unternehmen ergeben sich aus internen und externen Rahmenbedingungen. Die internen Anforderungen ergeben sich hauptsächlich aus dem Geschäftsinteresse des Unternehmens. Schwerpunkte sind hierbei das langfristige Bestehen des Unternehmens am Markt, die Wettbewerbsfähigkeit, die Rationalität sowie die Steigerung von Umsatz und Gewinn. Die Informationssicherheit als wichtiger Faktor für den Gesamterfolg eines Unternehmens ist hier nicht offensichtlich erkennbar. Durch das Bekanntwerden, den Verlust oder die unberechtigte Manipulation von unternehmensinternen Daten kann es jedoch zu Imageschäden, zum Verlust von Wettbewerbsvorteilen oder gar zur Beeinträchtigung der Funktionsfähigkeit von Unternehmensbereichen kommen.

Externe Anforderungen an die Informationssicherheit resultieren aus verschiedenen Gesetzen, Vorschriften und auch aus Verträgen. In diesem Zusammenhang sind beispielsweise als Grundlage die Artikel über die Persönlichkeit und Freiheit des Menschen im Grundgesetz zu nennen. Im Bereich Internet und elektronischem Handel sind insbesondere das Bürgerliche Gesetzbuch und das Handelsgesetzbuch relevant. Weiterhin sind das Informations- und Kommunikationsgesetz, das Gesetz zur Kontrolle und Transparenz in Unternehmen sowie das Signaturgesetz zu beachten. Die unzulässige Bekanntmachung, Verwertung oder Manipulation von Daten, die durch die genannten Gesetze geschützt sind, stellt einen Straftatbestand dar, der nach dem Strafgesetzbuch oder den Vorschriften des Bundesdatenschutzgesetzes geahndet wird. Darüber hinaus können sich zivilrechtliche Schadensersatzansprüche ergeben, die aus der Zuwiderhandlung gegen vertragliche Verpflichtungen mit Partnerunternehmen, Kunden, Lieferanten oder Versicherungen resultieren.

Aufgabe und Ziel der Informationssicherheit ist die Identifizierung und Erfüllung aller internen und externen Anforderungen an die Sicherheit von Informationen im Unternehmen. Hierzu müssen geeignete Sicherheits- und Schutzmaßnahmen entwickelt werden. Außerdem sind

Schäden, die durch vorsätzliches oder fahrlässiges Bekanntwerden, den Verlust oder die Manipulation von unternehmensinternen Informationen entstehen können, frühzeitig zu erkennen und auf ein Minimum zu reduzieren.

Die zunehmende Verbreitung von digitalen Dokumenten in Unternehmen führt zu neuen Anforderungen an die Informationssicherheit und verlangt entsprechend neuartige Sicherheitskonzepte. Die Kontrolle und Steuerung des Dokumentenflusses ist bezüglich analoger Dokumente leichter zu handhaben. Dokumente in Papierform sind direkt für jeden Betrachter sichtbar. Der jeweilige Aufbewahrungsort ist leicht festzustellen und zu überprüfen, sofern die Dokumente nicht absichtlich versteckt werden. Demgegenüber können digitale Dokumente – insbesondere unabsichtlich – wesentlich leichter an ungeeigneten bzw. ungesicherten Speicherorten abgelegt werden. Auch ist das Kopieren und die Verteilung digitaler Dokumente im Vergleich zum analogen Bereich schneller und einfacher möglich. Insbesondere können sensible Dokumente in digitaler Form das Unternehmen unbemerkt verlassen, wenn sie beispielsweise auf Diskette gespeichert oder per E-Mail versendet werden. Zu den Konzepten für Dokumenten- und Informationssicherheit in Unternehmen zählen das Vier-Augen-Prinzip und das Prinzip der Funktionstrennung. Diese organisatorischen Regelungen können durch technische Maßnahmen unterstützt werden, wie etwa Zugriffskontrollsysteme, Auditing, Datensicherungs- und Verfahren und gesicherte Übertragungswege.

Diese Konzepte und Maßnahmen bieten jedoch keinen ausreichenden Schutz vor unabsichtlicher oder fahrlässiger Verteilung von sensiblen Dokumenten durch einen berechtigten Empfänger. Ein großes Problem besteht darin, dass Dokumente von berechtigten Personen häufig an einem Ort gespeichert werden, wo sie für nicht-berechtigte Mitarbeiter zugreifbar sind. Dies ist z.B. dann gegeben, wenn Gehaltslisten für alle Mitarbeiter lesbar auf einem firmenintern zugänglichen Netzlaufwerk gespeichert sind. Die Datei entgleitet damit der Kontrolle des berechtigten Eigentümers. Natürlich gibt es in aktuellen Betriebssystemen die Möglichkeit, Rechte an einer Datei zu vergeben, doch dies wird häufig nicht getan, so dass eine regelmäßige Überprüfung angebracht ist. Zudem muss ein solches Speichern nicht bewusst erfolgen. Viele Programme legen automatisch temporäre Arbeitsdateien an, die anschließend nicht gelöscht werden oder nach einem Programmabsturz erhalten bleiben.

Durch das Speichern eines Dokumentes an einem ungeeigneten Ort werden Informationen öffentlich, ohne dass ein aktives Versenden erfolgte. Der im folgenden Abschnitt skizzierte Lösungsansatz hat das Ziel diesem Problem zu begegnen. Dazu wird periodisch für jeden Speicherort in einem Unternehmensnetz geprüft, ob sich dort ein Dokument befindet, dessen Vertraulichkeit dem Speicherort nicht angemessen ist.

5 Sicherheitspolitik für Dokumentenkontrolle

Die Grundlage eines Lösungsansatzes für die beschriebene Problemstellung der Dokumentensicherheit in Unternehmen ist eine spezifische Sicherheitspolitik für Dokumente, die einen Teil der globalen IT-Sicherheitspolitik darstellt, über die jedes Unternehmen verfügen sollte. Diese definiert auf allgemeiner Ebene die übergreifenden Ziele der Informationssicherheit eines Unternehmens.

Der hier beschriebene Lösungsansatz folgt dem Ansatz der Überwachung bzw. Überprüfung von Sicherheitsverstößen des Dokumentenflusses in Unternehmensnetzen. Auf solche Verstöße kann geeignet mittels Sicherheitspolitiken reagiert werden. Die Sicherheitspolitik für

Dokumente umfasst zunächst die Klassifikation von Dokumenten und Rechnern, Laufwerken bzw. Netzlaufwerken, d.h. allgemein von Speicherorten. Diese Klassifikation hat das Ziel, eine Einschätzung der Sensibilität eines Dokumentes bzw. der Vertrauenswürdigkeit eines Speicherorts zu liefern (vgl. Abschnitt 5.1). Darüber hinaus definiert die Sicherheitspolitik Regeln zur automatisierten Dokumentensteuerung. Diese Regeln dienen der automatisierten Bereinigung von Situationen, in denen ein sensibles Dokument in einem nicht vertrauenswürdigen Speicherort abgelegt wurde (vgl. Abschnitt 5.2). Schließlich enthält die Sicherheitspolitik organisatorische und technische Rahmenbedingungen sowie spezielle Handlungsanweisungen zum Umgang mit Dokumenten, die zur Durchsetzung des Gesamtkonzepts benötigt werden (vgl. Abschnitt 5.3).

Grundsätzlich sind diese Sicherheitspolitiken sehr detailliert ausgearbeitet und auf die spezifischen Bedürfnisse des Unternehmens angepasst. Eine Sicherheitsanalyse ist erforderlich, um typische Arbeitsabläufe zu erfassen und kritische Dokumentpfade aufzudecken. Bei der Modellierung der Sicherheitspolitiken bietet sich die Verwendung von Benutzergruppen und rollenbasierten Politiken an. Auch kann eine Klassifikation von Dokumenten und Speicherorten mit mehreren Parametern die Granularität erhöhen und so die Formulierung spezifischerer Sicherheitsregeln ermöglichen.

Im Rahmen dieses Artikels würde die Formulierung und Besprechung einer fein-granularen Sicherheitspolitik den Rahmen des Artikels übersteigen. Daher wird in den folgenden Abschnitten exemplarisch eine einfache Version einer Sicherheitspolitik dargestellt, die jedoch das Prinzip erläutert.

5.1 Klassifikation

Das in Tab. 1 dargestellte Klassifikationsschema für Dokumente umfasst vier verschiedene Sicherheitsstufen, die gegeneinander je nach dem Grad des potentiellen Schadens abgegrenzt werden, der für das Unternehmen durch den Verlust der Vertraulichkeit, Integrität und Verfügbarkeit von Dokumenten der jeweiligen Sicherheitsstufen entstehen könnte. Die Abgrenzung orientiert sich zudem am Umfang einer Störung, die als Folge des Verlusts oder der Verfälschung von Dokumenten zu erwarten ist, d.h. ob die Störung auf einen Funktionsbereich des Unternehmens beschränkt ist oder auch andere Bereiche von ihr betroffen sind.

Tab. 1: Exemplarisches Klassifikationsschema für Dokumente

Sicherheits-stufe	Einschätzung des Schadens bei Verlust bzw. Verfälschung	Aufwand der Wiederbeschaffung	Störung von Funktionsbereichen
0	Kein Schaden.	Ohne Aufwand.	Keine.
1	Geringe Schäden.	Geringer Aufwand.	Unerhebliche Störungen.
2	Deutliche Schäden, jedoch auf den Verantwortungsbereich der jeweiligen Funktionsbereiche beschränkt.	Erheblicher Aufwand.	Deutliche Störung des verantwortlichen Bereichs, keine Störung anderer Bereiche.
3	Deutliche Schäden, die über den Verantwortungsbereich der jeweiligen Funktionsbereiche hinausgehen.	Erheblicher Aufwand.	Deutliche Störung des verantwortlichen Bereichs, Störung anderer Bereiche.

Das Klassifikationsschema für Speicherorte ist in Tab. 2 abgebildet. Die in der Tabelle erwähnten Sicherheits- und Sicherungsmechanismen beziehen sich auf technische Maßnahmen wie Zugriffsschutz, Absicherung durch Firewalls, Verschlüsselungs- und Backupmechanismen, mit denen die Rechner und Laufwerke der jeweiligen Sicherheitsstufen abgesichert sind. Die Einstufung der Sicherheit ergibt sich aus dem Umfang der Sicherheitsmaßnahmen.

Tab. 2: Exemplarisches Klassifikationsschema für Speicherorte

Sicherheits-stufe	Sicherheits-mechanismen	Einstufung der Sicherheit	Speicherung folgender Dokumente erlaubt
0	Keine	Unsicher.	Sicherheitsstufe 0.
1	Grundlegende	Bedingt sicher.	Sicherheitsstufe 0 und 1.
2	Ausreichend	Sicher.	Sicherheitsstufe 0, 1 und 2.
3	Umfangreich	Sicher und vertrauenswürdig.	Sicherheitsstufe 0, 1, 2 und 3.

Ebenso wie bei der Klassifizierung der Dokumente ist auch bei der Einstufung der Speicherorte auf eine einfache Erweiterungs- bzw. Änderungsmöglichkeit der Einstufung zu achten. Je nach Anwendung können andere Vertrauensstufen oder eine feinere Untergliederung angebracht sein. Grundsätzlich ist vorab in einer Sicherheitsanalyse zu untersuchen, ob die Klassifizierung von Dokumenten und Speicherorten ausreichend ist, um die Sicherheitsanforderungen von Unternehmen abzudecken bzw. sinnvoll zu ergänzen.

Beispielhaft soll hier eine komplexe Unternehmensstruktur betrachtet werden, die sich sicherlich auch in der Netzwerkstruktur und den Zugriffsberechtigungen niederschlägt. Gemäß der Unternehmenssicherheitspolitik darf die Personalabteilung nicht auf die Dokumente der Entwicklungsabteilung zugreifen können und umgekehrt. Die Dokumente der Personalabteilung werden stets in die Sicherheitsstufe 2 eingeordnet, ebenso Dokumente aus der Konstruktionsabteilung. Werden Dokumente aus diesen beiden Abteilungen an Speicherorten der Sicherheitsstufe 2 oder 3 der jeweils anderen Abteilung abgespeichert, kann anhand des hier vorgestellten Lösungskonzeptes dies nicht als Sicherheitsverstoß erkannt werden. Hier zeigen sich die Grenzen dieser exemplarischen Klassifikation. Eine detailliertere Ausarbeitung, zugeschnitten auf die spezifischen Gegebenheiten des Unternehmens, ist angebracht.

5.2 Automatisierte Dokumentensteuerung

Die automatisierte Dokumentensteuerung soll gewährleisten, dass die von der Sicherheitspolitik aufgestellten Bedingungen (siehe Tab. 2, letzte Spalte) möglichst zu jedem Zeitpunkt erfüllt sind. Verstöße gegen diese Bedingungen müssen schnell aufgedeckt und geeignete Maßnahmen eingeleitet werden. Die anzuwendenden Maßnahmen sind ebenfalls in der Sicherheitspolitik einer Organisation festgelegt. Um auf Regelverstöße effizient und zeitnah zu reagieren, ist eine automatische Auslösung wünschenswert. In Abschnitt 6 wird dargestellt, wie ein agentenunterstützter Durchsetzungsmechanismus aussehen kann.

Fasst man die Summe der Randbedingungen zusammen, lassen sich daraus allgemeine Regeln ableiten. Die exemplarische Politik in Tab. 2 lässt sich mit folgender Regel beschreiben:

1. Die Sicherheitsstufe von Dokumenten muss kleiner oder gleich der des Speicherorts sein, auf dem sie gespeichert sind.

Weiterhin werden Regeln benötigt, die zu jeder Zeit die Konsistenz des Konzepts garantieren, falls ein Dokument oder ein Speicherort unklassifiziert ist. Ein erster Ansatz für solche Regeln könnte sein:

2. Alle nicht klassifizierten Dokumente werden automatisch mit der Sicherheitsstufe 2 gekennzeichnet.
3. Alle nicht klassifizierten Speicherorte des Unternehmensnetzes werden automatisch mit der Sicherheitsstufe 0 versehen.

Falls bei der Überprüfung eines Speicherorts Verstöße gemäß Regel 1 festgestellt werden, wird je nachdem, wie schwerwiegend der Verstoß eingeschätzt wird, automatisch eine geeignete Maßnahme ergriffen. Die notwendige Einschätzung kann nach der folgenden Regel geschehen:

4. Bei einer Differenz der Sicherheitsstufe des betrachteten Dokumentes und der Sicherheitsstufe des zugehörigen Speicherorts
   - von *eins* wird der Verstoß als akzeptabel eingestuft und lediglich ein entsprechender Eintrag für das Reporting generiert.
   - von *zwei* wird der Verstoß als kritisch eingestuft. Das Dokument wird in diesem Fall verschlüsselt, um die Missbrauchsmöglichkeiten einzuschränken.
   - von *drei* wird der Verstoß als nicht akzeptabel eingestuft. Das Dokument wird in einen gesicherten Bereich verschoben und es wird eine Untersuchung eingeleitet, wie es zu diesem Sicherheitsvorfall kommen konnte.

Wiederum ist diese Reaktion beispielhaft und ist selbstverständlich an die Sicherheitspolitik des jeweiligen Unternehmens anzupassen.

5.3 Rahmenbedingungen und Handlungsanweisungen

Um die Sicherheitspolitik für Dokumente in der Unternehmenspraxis erfolgreich umsetzen zu können, müssen einige organisatorische Rahmenbedingungen erfüllt sein. Für die initiale Klassifikation von Dokumenten und Speicherorten muss eine eindeutige Verantwortlichkeit definiert sein. Hierbei liegt es nahe, die Verantwortung dem Funktionsbereich zuzurechnen, der auch für die betroffenen Daten verantwortlich ist. Weiterhin impliziert jede Änderung des Ausgangsdokumentes eine Überprüfung und gegebenenfalls eine Anpassung der Einstufung des Dokumentes, wenn z.B. vertrauliche Informationen angefügt werden. Zudem können auch externe Bedingungen die Klassifikation eines Dokumentes ändern, bspw. wenn der Quartalsbericht eines börsennotierten Unternehmens veröffentlicht wird oder wenn die Gültigkeit eines eigenen Patents abläuft. Die Nachführung der Einstufung muss technisch möglich sein und ist organisatorisch zu regeln.

Außer der Handhabung von Dokumenten ist ein Meldeprozess zu definieren und zu implementieren, der geeignete Aktionen festlegt, die im Fall eines akzeptablen Verstoßes durchzuführen sind. Dieser Prozess sollte auch berücksichtigen, dass in Abhängigkeit des betroffenen Dokumentes oder Organisationsbereiches unterschiedliche Personen informiert werden müssen.

Neben den Klassifizierungen und den Regelungen bei Verstößen sind Handlungsanweisungen für die tägliche Arbeit der Benutzer mit klassifizierten Dokumenten wichtig. Diese müssen mindestens die folgenden Prozesse umfassen:

- Kopiervorgänge,
- Bearbeitung von Dokumenten,
- Übertragung via Post, Fax und E-Mail,
- Weitergabe via Sprache,
- Ausdruck von Dokumenten,
- Ablage in herkömmlichen und digitalen Archiven,
- sowie die Zerstörung von Dokumenten und Informationen.

Die Entwicklung dieser Handlungsanweisungen erfordert a priori eine umfangreiche unternehmensspezifische Ist-Aufnahme und Ist-Analyse.

6 Realisierung

In diesem Abschnitt soll ein geeigneter technischer Lösungsansatz präsentiert werden, der die Distributionskontrolle von Dokumenten automatisiert. Wir schlagen den Einsatz von mobilen Überwachungsagenten vor. Mobile Agenten können in dieser spezifischen Umgebung ihre technischen Vorzüge effektiv einbringen.

Die IT-Infrastruktur eines Unternehmens ist typischerweise sehr verteilt. Es gibt dedizierte Server für Datenhaltung, Webseiten und Mail-Handhabung. Weiterhin verfügen die Mitarbeiter über eigene Arbeitsplatzrechner und mobile Endgeräte. Produktivsysteme für Workflow- und Dokumentenmanagement kommen noch hinzu.

Mobile Agenten können sich auf jeden dieser Rechner begeben – eine dort installierte Ablaufumgebung vorausgesetzt. Sie greifen lokal auf gespeicherte Daten zu und verursachen dadurch keinen Netzwerkverkehr. Zudem können auch Dateibereiche untersucht werden, die nicht als Netzwerklaufwerk für andere Rechner zugreifbar sind. Auch die Verarbeitungsgeschwindigkeit steigt, da lokale Leseoperationen effektiver sind als der Datendurchsatz eines Netzwerkes.

Ein weiterer Vorteil ist die leichte Anpassung des Systems an neue Gegebenheiten. Da durch den Agenten der Code zu den Daten transportiert wird, können ganz einfach neue Wasserzeichenalgorithmen verwendet oder eine inhaltsbasierte Suche „nachgerüstet“ werden.

Zudem ist die Verwendung von verteiltem Code die natürliche Antwort auf verteilte Datenhaltung. Bei Verwendung mehrerer Agenten wird die Verarbeitung ohne besonderen Aufwand ebenfalls verteilt parallelisiert. Mobile Agenten erlauben darüber hinaus auf einfache Weise die logische Kombination von Datenbeständen, auch wenn deren Zusammenführung beim Ablegen der Daten nicht geplant war [PPHG02].

Um die Distributionskontrolle von Dokumenten zu gewährleisten, wird die jeweilige Sicherheitseinstufung eines Dokumentes mit Hilfe eines geeigneten digitalen Wasserzeichenverfahrens in das Dokument selbst eingebracht und somit fest mit diesem verbunden. Weiterhin wird jeder Speicherort des Unternehmensnetzes mit einer Sicherheitseinstufung gekennzeichnet. Ein mobiler Agent – im weiteren Überwachungsagent genannt – hat die Aufgabe, Verstöße gegen die Sicherheitspolitik aufzudecken. Dazu wird eine Gruppe von Überwachungsagenten erzeugt. Die vorhandenen Speicherorte werden unter den Agenten aufgeteilt. Jeder Agent besucht nun nacheinander die ihm zugeordneten Systeme und untersucht jeweils das lokale Dateisystem. Aus jedem Dokument wird das Wasserzeichen ausgelesen um dessen Si-

cherheitsklassifikation zu ermitteln. Die Sicherheitsstufe der Dokumente kann nun mit der Einstufung des Speicherorts verglichen werden. Aus diesem Vergleich leitet der mobile Überwachungsagent im Bedarfsfall gemäß den Regeln der Sicherheitspolitik geeignete Maßnahmen ab. Nachdem der Überwachungsagent seine Arbeit auf einem Rechner beendet hat, migriert er auf den Rechner im Unternehmensnetz.

Natürlich kann ein Überwachungsagent beliebig komplex gestaltet werden. So könnte man dem Agenten ermöglichen, Erfahrungswerte früherer Besuche von Rechnern bei der Wegewahl einzubeziehen. Der Agent könnte auch Prüfsummen über bereits geprüfte Dokumente bilden um bei einem späteren Besuch nur die geänderten Dokumente zu untersuchen. Weiterhin erlaubt die Kommunikation zwischen Agenten den Abgleich der einzelnen Suchaufträge. So könnten bspw. auch Dubletten von Dokumenten gefunden werden.

Da der Agent eine wesentliche Maßnahme zur Durchsetzung der Unternehmenspolitik darstellt, sind geeignete Maßnahmen zu treffen, die ein versehentliches oder absichtliches Unterminieren dieser Maßnahme durch die Mitarbeiter unmöglich machen:

- Agenten dürfen nicht abgefangen, blockiert oder manipuliert werden.
- Agenten dürfen keine Informationen von einem Speicherort mitnehmen.
- Die Agentenplattform auf zu untersuchenden Rechnern darf nicht deaktiviert werden.
- Es dürfen keine neuen Speicherorte geschaffen werden.
- Dem Agenten ist Zugriff auf alle Dateibereiche zu gewähren.
- Die Privatsphäre der Mitarbeiter ist angemessen zu berücksichtigen.

Um diese Anforderungen zuverlässig und verbindlich umzusetzen, ist ein Agentensystem erforderlich, mit dem sich die sicherheitstechnischen Anforderungen durchsetzen lassen. Es existieren grundsätzlich vier mögliche Angriffsszenarien [RoJa01]:

a) ein Agent schadet einem Agentenserver
b) ein Agent schadet einem anderen Agenten
c) ein Agentenserver schadet einem Agenten, und
d) ein Dritter schadet einem Agenten während dessen Übertragung

Ein ausgereiftes Sicherheitsmodell muss mit diesen und weiteren Bedrohungen umgehen können, damit diese Technologie im beschriebenen Szenario sinnvoll eingesetzt werden kann.

Es gibt eine Vielzahl von Agentenplattformen, die sich auf unterschiedliche Aspekte der Agententechnologie konzentrieren, vgl. z.B. [LaOs98], [BePR00] und [BrER00]. Eine Plattform, die sich auf Sicherheit spezialisiert, ist die Agentenplattform SeMoA (Secure Mobile Agents) [RoJa01] [PPHG02]. SeMoA ist als Open Source Projekt verfügbar und stellt Mechanismen zur Absicherung von mobilen Agenten bereit.

Die elektronische Signatur stellt dabei ein wichtiges Instrument bereit, um Agenten rechtsverträglich zu gestalten. Um die Autorisation für den Zugriff auf lokale Ressourcen zu bestimmen, muss der Auftraggeber des Agenten nicht-abstreitbar ermittelt werden können. Dazu verwendet SeMoA die elektronische Signatur. Jeder Agent wird zweifach signiert: zum einen der Programmcode des Agenten und in einer getrennten Signatur die gesammelten Daten und der Zustand des Agenten. Das Format digitaler Signaturen ist das PKCS#7 Format, ein Standard für kryptographische Nachrichten, der auf ASN.1, X.501 und X.509 aufbaut.

Diese Signaturen sind eine wichtige Voraussetzung für die Implementierung von Sicherheitspolitiken, gegen die der Agentenserver neu ankommende Agenten prüft. Ergebnis der Prüfung ist entweder das Abweisen des Agenten oder die Ausstattung mit Rechten, die für seine spezifische Aufgabe benötigt werden. Anschließend kann der Agent seine Aktion beginnen.

Die Gesamtarchitektur der Dokumentenflusskontrolle sollte einen zentralen Agentenserver vorsehen, der die regelmäßige Aktivierung der Agenten kontrolliert und als Heimatserver fungiert. Dort sind auch die Konfiguration und die Weiterverarbeitung der Reporte angesiedelt.

Nach dem Start migriert der Agent wie beschrieben sukzessive zu den zu untersuchenden Datenquellen, durchsucht die lokalen Datenspeicher und vergleicht markierte Dokumente mit der Klassifikation des Speicherortes. Die Verschlüsselung des Dokumentes kann der Agent vor Ort vornehmen. Dazu generiert der Agent einen zufälligen Schlüssel für einen vorab gewählten Algorithmus, mit dem der Agent die Datei verschlüsselt. Unmittelbar vor der Verschlüsselung kommuniziert der Agent den Schlüssel an den zentralen Agentenserver, auf dem er gestartet worden ist. Dieser archiviert den Schlüssel mit dem das Dokument wieder entschlüsselt werden kann. So ist gewährleistet, dass der Agent nicht versehentlich verloren geht und das verschlüsselte Dokument nicht mehr zugreifbar ist.

Das Erstellen der Reporte kann durch den Agenten erledigt werden. Nach Beendigung der lokalen Suche fasst er die gefundenen Regelverstöße und die ergriffenen Maßnahmen zusammen. Am Schluss seines Auftrags kehrt er auf den Heimatserver zurück und übergibt diesem seinen Report. Der Server kann die Reporte vieler parallel gestarteter Agenten nochmals zusammenführen und die Benachrichtigung der zuständigen Funktionsträger durchführen. Hier bietet sich E-Mail als asynchrones Kommunikationsmedium an.

7 Zusammenfassung und Ausblick

Der in diesem Artikel skizzierte Lösungsansatz der Dokumenten- und Informationssicherheit weist im Wesentlichen zwei neuartige Aspekte auf. Zum einen werden Dokumente mit der ihr zugeordneten Sicherheitsinformationen untrennbar verbunden, so dass eine Überprüfung der Sicherheitspolitik unabhängig vom Speicherort und ggf. sogar von der Form des Dokumentes (digital oder analog) möglich wird. Zum anderen läuft die Prüfung der Sicherheitspolitik durch den Einsatz von mobilen Agenten und einer automatisierten Dokumentensteuerung weitgehend automatisiert ab, so dass Sicherheitslücken möglichst zeitnah erkannt und geschlossen werden können. Die Auswirkungen von Fehlern, die auf menschliches Versagen zurückzuführen sind, können somit weitgehend ausgeschlossen werden.

Der Einsatz des dieser Technologie ist komplementär zu traditionellen Schutzmechanismen des Zugriffsschutzes und der Vertraulichkeit, wie etwa die konsequente Verschlüsselung von vertraulichen Dokumenten. Bspw. besteht bezüglich der Verschlüsselung von Dokumenten generell die Gefahr, dass ursprünglich verschlüsselte Dokumente ordnungsgemäß entschlüsselt und anschließend versehentlich ungeschützt abgelegt werden. In diesem Fall ermöglicht der zusätzliche Einsatz des mobilen Überwachungsagenten eine Überprüfung der Sicherheitspolitik und eine zeitnahe Reaktion auf Verletzung der Sicherheitspolitik. Die automatische Klassifizierung von nicht markierten Dokumenten etabliert einen Grundsicherheitsstandard, der nicht umgangen werden kann.

Wichtig für die Einführung eines solchen Systems ist die organisatorische Verankerung der notwendigen Funktionsträger und Abläufe im Unternehmen. Nach wie vor ist eine Sensibili-

sierung der Mitarbeiter für die Gefahren, die durch fehlgeleitete Dokumentenflüsse entstehen, der beste Schutz.

Die Arbeiten, die diesem Artikel zu Grunde liegen, werden im Rahmen des Projektes SicAri durch das Bundesministerium für Bildung und Forschung gefördert.

Literatur

[ArSW03] M. Arnold, M. Schmucker, S. Wolthusen: Techniques and Applications of Digital Watermarking and Content Protection, Artech House (2003), ISBN 1-58053-111-3.

[BePR00] F. Bellifemine, A. Poggi, G. Rimassa: Jade Programmers Guide. Technischer Bericht. Juni 2000.

[Brau99] P. Braun: Über die Migration bei Mobilen Agenten. In: Jenaer Schriften zur Mathematik und Informatik 13 (1999).

[BrER00] P. Braun, C. Erfurth, W. R. Rossak: An Introduction to the Tracy Mobile Agent System. Technical Report No. 2000/24, Friedrich Schiller Universität Jena, September 2000.

[BuKZ98] S. Burgett, E. Koch, J. Zhao: Copyright Labeling of Digitized Image Data. In: IEEE Communications Magazine, März 1998, Vol. 36, No. 3.

[CKLS97] I.J. Cox, J. Kilian, T. Leighton, T. Shamoon: Secure Spread-Spectrum Watermarking for Multimedia, IEEE Transactions on Image Processing, 1997.

[CKM+01] R. S. Cost, S. Kallurkar, H. Majithia, C. Nicholas, Y. Shi: Integrating Distributed Information Sources with CARROT II. Proceedings of the 6th International Workshop on Cooperative Information Agents VI, 2002, ISBN 3-540-44173-5.

[KoZh95] E. Koch, J. Zhao: Towards Robust and Hidden Image Copyright Labeling. In: Proceedings of the IEEE Workshop on Nonlinear Signal and Image Processing, June 1995, Halkidiki, Greece.

[LaOs98] D. B. Lange, M. Oshima: Programming and Deploying Java Mobile Agents with Aglets.Peachpit Press (1998), ISBN 0201325829.

[LaOs99] D. B. Lange, M. Oshima: Seven Good Reasons for Mobile Agents. In: Communications of the ACM, Vol. 42, Nr. 3, 1999.

[PiBu03] U. Pinsdorf, Ch. Busch. Neue Potenziale für mobile Dienstleistungen – Einsatz von mobilen Agenten im mobilen Arbeitsumfeld. In: M. Weiss, Ch. Busch, W. Schröter: Multimedia Arbeitsplatz der Zukunft. Assistenz und Delegation mit mobilen Softwareagenten. Talheimer Verlag (2003). ISBN 3-89376-105-5.

[PPHG02] U. Pinsdorf, J. Peters, M. Hoffmann, P. Gupta: Context-aware Services based on Secure Mobile Agents. In: Proceedings of 10th International SoftCOM Conference, Oktober 2002. IEEE Communication Society. ISBN 953-6114-52-6.

[RoJa01] V. Roth, M. Jalali: Concepts and Architecture of a Security-centric Mobile Agent Server. In: Proc. Fifth International Symposium on Autonomous Decentralized Systems (ISADS 2001), Dallas, Texas, U.S.A., March 2001. IEEE Computer Society Press.

[Roth01] V. Roth: Sichere verteilte Indexierung und Suche von digitalen Bildern. Dissertation, Technische Universität Darmstadt (2001).

[Uspa97] U.S. Patent and Trademark Office: System and Method for Distributed Computation Based upon the Movement, Execution and Interaction of Processes in a Network. US patent no. 5603031.

[WoJe95] M. Woolridge, N. Jennings: Intelligent Agents: Theory and Pratice. In: Knowledge Engineering Review 10 (1995), Nr. 2.

[ZhKo95] J. Zhao, E. Koch: Embedding Robust Labels into Images for Copyright Protection. In: Proceedings of the KnowRight'95 Conference, August 1995, Wien, R. Oldenbourg.

[ZhLu99] J. Zhao, C. Luo: Digital Watermark Mobile Agents. In: Proceedings of 22nd National Information Systems Security Conference, Oktober 1999.