Technische Universität Kaiserslautern

Lehrgebiet Datenverwaltungssysteme

Seminar: *Grundlagen webbasierter Informationssysteme*

Thema: *Trust, Reputation, Privacy*

Bearbeiter:

Rafael Schirru

Betreuer:

Prof. Dr. Ing. Stefan Deßloch

Kaiserslautern, den 25.06.2004

Gliederung

1. Einleitung

Trust und *Trust Management* sind wichtige Elemente der Entscheidungsgrundlagen im E-Commerce, bei Internet-Interaktionen und elektronischen Vertragsverhandlungen. Ziel ist es, Methoden zur Verfügung zu stellen, die es Geschäftspartnern erlauben, trotz des nicht vorhandenen persönlichen Kontaktes bei Internet-Geschäftstransaktionen, eine Vertrauensbeziehung aufzubauen. Nach Blaze et. al. wird Trust Management wie folgt definiert: „a unified approach to specifying and interpreting security policies, credentials, relationships which allow direkt authorisation of security-critical actions“ [GrSl03]. Nach der Gegenüberstellung zweier Definitionen des Begriffes Trust werden zu diesem Zweck die von IBM und Microsoft entwickelten Modelle WS-Trust und WS-Federation vorgestellt.

Neben dem Aufbau von Vertrauensbeziehungen spielen Fragen der *Reputation* von Dienstanbietern für Interaktionen im Internet eine wichtige Rolle. Für Dienstnutzer stellen sich Fragen nach der Zuverlässigkeit von Informationen, beispielsweise von selbsterklärten Experten bei expertcentral.com, oder danach, ob ein Verkäufer bei eBay seine Ware angemessen beschreibt und versendet. Nach der Betrachtung unterschiedlicher Definitionen von Reputation in der Informatik wird eine Klassifikation von Reputationsarten dargestellt. Anhand des Auktionshauses eBay wird anschließend beispielhaft die Relevanz von Reputationssystemen in der Praxis verdeutlicht. Abschließend zum Thema Reputation wird mittels des EigenTrust-Algorithmus aufgezeigt, wie Trust auf der Grundlage von Reputation etabliert werden kann.

Als dritter Aspekt, der bei Interaktionen im Internet von Bedeutung ist, ist der Datenschutz (*Privacy*) zu nennen. Dienstnutzer sind häufig besorgt, welche Informationen sie preisgeben, während sie online sind, und wer schließlich Zugang zu diesen Informationen erhält. Ziel ist es, dem Benutzer die Möglichkeit zu geben, ohne großen Aufwand selbst zu entscheiden, welche persönlichen Informationen er bekanntgeben bzw. geheimhalten möchte. Zu diesem Zweck wird das P3P-Protokoll vorgestellt, das einerseits einen Standard für die computergestützte Verarbeitung von Privacy Policies bietet und andererseits die automatische Verarbeitung von Privacy Policies mittels Benutzeragenten (z.B. Web-Browser) ermöglicht.

2. Trust

2.1. Operationale Trust-Definition vs. Trust als interner Zustand

Die Wichtigkeit von Trust bzw. Trust Management kommt laut [GrSl03] einerseits durch die große Anzahl an Forschungsarbeiten, die in den letzten Jahren zu diesem Thema durchgeführt

wurden, andererseits durch die Bemühungen führender Hardware- und Softwareverkäufer Trust Management in ihre Produkte zu integrieren, zum Ausdruck. Die Motivation, welche hinter diesen Bemühungen steckt, ist in der großen Bedeutung von Vertrauen (Trust) für Geschäftstransaktionen im Internet zu sehen. Da das Vertrauen nicht über den persönlichen Kontakt aufgebaut werden kann, müssen Methoden entwickelt werden, welche es ermöglichen Vertrauen zu etablieren.

Im Folgenden soll nun eine Definition des Begriffes Trust in Anlehnung an [Camp02] erfolgen. Dazu werden zwei verbreitete Definitionen von Trust gegenübergestellt: die operationale Variante und die Definiton von Trust als interner Zustand.

In der *operationalen Definition* wird vorausgesetzt, dass die beteiligten Parteien auf Grundlage von Kenntnissen über mögliche Belohnungen für das Vertrauen bzw. Nichtvertrauen Entscheidungen treffen. Wird einer Partei vertraut, so kann zusätzliches Vertrauen durch eine dann zu Stande kommende Interaktion hinzugewonnen werden, bei Nichtvertrauen wird der Verlust von bereits aufgebautem Vertrauen vermieden, da es nicht zur Interaktion zwischen den Parteien kommt. Die Vermeidung von Risiken spielt in der operationalen Definition von Trust eine entscheidende Rolle. Auch in der Spieltheorie wurde Trust aus operationaler Sicht untersucht. Es ist zu beachten, dass hier die Kompetenz einer Partei zur Lösung eines Problems keine Rolle spielt, wenn es darum geht, ob und wieviel Vertrauen dieser Partei entgegengebracht wird. Für Vertrauensbeziehungen im Internet muss sowohl die Absicht einer Partei als auch ihre Problemlösungskompetenz berücksichtigt werden. Dabei ist insbesondere das Feststellen der Absicht einer beteiligten Partei problematisch, da viele Internetseiten unpersönlich sind und somit die Ziele die sie verfolgen schwer identifiziert werden können.

Im Kontext der operationalen Definiton des Begriffes Trust spielt jene Variante eine entscheidende Rolle, die das Vertrauen auf Grundlage von Eigeninteressen der Partei, der vertraut wird, etabliert. Diese Variante des Begriffes Trust setzt den wirtschaftlich denkenden Menschen (homo economicus) voraus. Es müssen Informationen über die Partei, der vertraut wird, zur Verfügung gestellt werden, so dass überprüft werden kann, ob ihre Interessen mit den Interessen der Partei, die das Vertrauen entgegebringt, übereinstimmen. Für Anwendungen im Internet bedeutet dies, dass seitens eines Dienstanbieters die Motivation vorausgesetzt wird, die Sicherheit seines Dienstes zu gewährleisten und den Datenschutzanforderungen der Dienstnutzer gerecht zu werden. Sind diese Voraussetzungen gegeben, so äußert sich das entgegengebrachte Vertrauen des Dienstnutzers dadurch, dass er bereit ist persönliche Informationen zu teilen.

Die zweite Definition des Begriffes betrachtet *Trust als internen Zustand*. Dabei schätzt die Partei, die Vertrauen entgegenbringt, die Motivation der Partei, der sie Vertrauen entgegenbringt, ein. Strukturierte Interviews und Umfragen, durchgeführt von Sozialpsychologen, führten zu dem Ergebnis, dass eine starke Verbindung zwischen dem

entgegengebrachten Vertrauen und dem Kooperationswillen existiert. Zwar kann Trust nicht als der Wille zur Kooperation mit einer Partei definiert werden, jedoch bedingen sich Trust und Kooperationswille gegenseitig.
Im Vergleich ergibt sich, nach [Camp02], dass Trust nach der operationalen Definition auf das messbare Risiko, welches sich statistisch oder deterministisch nachweisen lässt, abzielt, wohingegen Trust als interner Zustand das wahrgenommene Risiko zum Gegenstand hat.
Anhand eines Beispiels soll dieser Unterschied verdeutlicht werden: Es soll das Risiko betrachtet werden, welches aus dem Bekanntwerden persönlicher medizinischer Daten resultieren kann. In den USA besteht das Risiko für eine Person, deren medizinische Daten in die Hände dritter gelangen darin, dass sie ihren Arbeitsplatz oder ihre Krankenversicherung verliert. Das Risiko im United Kingdom hingegen beschränkt sich auf den Verlust des Arbeitsplatzes. Wird die operationale Definition des Begriffes Trust zu Grunde gelegt, so kann eindeutig gesagt werden, dass der Schutz medizinischer Daten in den US wichtiger ist als im UK, da das Risiko bei Missbrauch größer ist. Legt man jedoch die Definition von Vertrauen als internen Zustand zu Grunde, so sind die Risiken, unter der Voraussetzung, dass in beiden Kulturen die gleiche Sensibilität für den Schutz medizinischer Daten herrscht, in etwa gleich hoch zu bewerten.
Um Vertrauensbeziehungen (z.B. In P2P-Netzen) zu etablieren und beobachtetes Verhalten zu verstehen ist es wichtig beide Perspektiven des Begriffes Trust zu kennen.

2.2. WS-Trust

Bedingt durch den fehlenden persönlichen Kontakt bei Geschäftsbeziehungen im Internet werden Methoden benötigt, welche die Etablierung von Vertrauen (Trust) zwischen Geschäftspartnern ermöglichen. Ziel von WS-Trust und WS-Federation ist es dabei, den individuellen Sicherheitsbedürfnissen der Dienstnutzer und Dienstanbieter gerecht zu werden. Das Risiko, dass Agenten Dienste nutzen, zu denen ihnen die Berechtigung fehlt, soll dabei im Sinne der operationalen Definition des Begriffes Trust, minimiert werden. Darüber hinaus soll Interoperabilität für Anwendungen in heterogenen Systemen ermöglicht werden, so dass Organisationen auf Grundlage ihrer bereits vorhandenen Sicherheitstechnologien Trust-Bündnisse eingehen können.
Web Service Trust (WS-Trust) beschreibt ein Modell, mit dessen Hilfe sowohl direkte als auch vermittelte Trust-Beziehungen aufgebaut werden können. Nachfolgend wird in Anlehnung an [IBMi02] dargestellt, wie direkte Trust-Beziehungen aufgebaut bzw. als Basis für vermittelten Trust mit Hilfe von Security Token Issuance Services genutzt werden können.
Da zum Aufbau einer Trust-Beziehung der Austausch von Security Token von zentraler

Bedeutung ist, soll an dieser Stelle das in [IBMi02] vorgestellte Security Token Service Model kurz erläutert werde. Ein *Security Token* beinhaltet Informationen, welche für sicherheitskritische Aktionen (z.B. das Anmelden bei einem Web Service) relevant sind.
Der Austausch von Security Token findet zwischen drei Instanzen statt: dem Dienstnutzer, dem Web Service sowie dem Security Token Service. Abb.1 veranschaulicht diesen Sachverhalt. Zu erwähnen bleibt, dass der Security Token Service selbst als Web Service realisiert werden kann. Nachdem ein Dienstnutzer bzw. Web Service dem Security Token Service ein von ihm benötigtes Security Token vorgelegt haben, stellt dieser dem Dienstnutzer bzw. Web Service das geforderte Security Token aus.
Eine *direkte Trust-Beziehung* kann mittels *Benutzername und Passwort* unter Verwendung des TLS Protokolls (Transport-Level Security) etabliert werden. Dabei wird vorausgesetzt, dass die beiden Parteien über ein geteiltes Geheimnis (nämlich das Passwort des Benutzers) verfügen. Anhand eines Beispiels soll dieser Mechanismus verdeutlicht werden: Der Benutzer öffnet eine sichere Verbindung zu einem Web Service mittels TLS. Seiner Anfrage ist ein Security Token, welches seinen Benutzernamen und sein Passwort enthält, beigefügt. Nachdem der Web Service das Token authentisiert hat, verarbeitet dieser die Anfrage und gibt das Ergebnis zurück. Es ist zu beachten, dass über das Verhältnis zwischen den beiden Parteien (Diensterbringer und Dienstnutzer) keine Annahmen getroffen werden.
Eine weitere Möglichkeit eine direkte Trust-Beziehung aufzubauen besteht in der Benutzung von Security Token, denen ein Web Service direkt Vertrauen (Trust) entgegenbringt. Das Security Token des Senders (oder dessen Stellvertreters, z.B. eine unterzeichnende Autorität) ist dem Web Service dabei bekannt und wird als vertrauenswürdig eingeschätzt. Im Gegensatz zur Etablierung von Trust mittels Benutzername und Passwort wird in dieser Variante vorausgesetzt, dass bereits eine Trust-Beziehung zwischen den beiden Parteien existiert, welche die Grundlage für die Benutzung des Security Tokens darstellt. Diese Trust-Beziehung könnte manuell (durch Konfiguration einer Anwendung) oder durch den gesicherten Austausch von Schlüsseln aufgebaut worden sein. Folgendes Szenario soll diese Variante veranschaulichen: Der Sender schickt eine Nachricht, welche ein signiertes Security Token enthält, zu einem Web Service. Im Gegensatz zum gewöhnlichen, zeichnet sich das signierte Security Token dadurch aus, dass die in ihm enthaltenen Erklärungen von seinem Herausgeber (kryptographisch) bestätigt werden. Zum Beispiel kann der Sender mittels einer Signatur nachweisen, dass er rechtmäßiger Besitzer dieses Tokens ist. Der Service überprüft den Nachweis und wertet sodann das Security Token aus. Handelt es sich um eine gültige Signatur und besteht direktes Vertrauen zu dem Token, so wird die Anfrage des Senders verarbeitet und deren Ergebnis zurückgeliefert. Die direkte Etablierung von Trust mittels Security Tokens trifft ebenfalls keine Annahme über das Verhältnis zwischen den beteiligten Parteien.
In den oben genannten Varianten zur Etablierung einer Trust-Beziehung zwischen dem Nutzer

und dem Anbieter eines Web Services werden die relevanten Informationen über den Nutzer direkt, in Form eines Security Tokens, an die Nachricht angehängt. Eine weitere Möglichkeit Zugang zu diesen Informationen zu erhalten besteht in der Verwendung *referenzierter Security Token*. Dabei wird das Token nicht als Teil der Nachricht übermittelt, statt dessen stellt der Nutzer eine Referenz zur Verfügung, bei der das Token erworben werden kann. Ein Szenario könnte dabei wie folgt aussehen: Der Dienstnutzer sendet eine Anfrage an den Web Service, welche die Referenz zu einem Security Token und dessen Eigentumsnachweis enthält. Mit dieser Information kann der Web Service das Token bei einem Token Store Service abfragen und überprüfen. Vertraut der Web Service dem Security Token, so wird die Anfrage des Dienstnutzers bearbeitet und das Resultat an den Nutzer übermittelt.
In einem nächsten Schritt soll nun die *Authentisierung durch eine vertrauenswürdige Instanz* betrachtet werden. Diese Form des Aufbaus einer Trust-Beziehung spielt immer dann eine Rolle, wenn ein Web Service ein Security Token eines bestimmten Typs (im Beispiel der Nachweis der Identität) zur Authentisierung voraussetzt. Dazu nimmt der Dienstnutzer zunächst Kontakt zu einem Security Token Service auf, um ein Security Token zu erhalten, welches ihm die vom Web Service benötigten Informationen attestiert (hier: seine Identität). Dieses sendet er, zusammen mit seiner Anfrage, an den Web Service, dessen Dienst er auf diese Weise nutzen kann. Es ist zu beachten, dass gegebenenfalls bereits existierende Sicherheitsprotokolle benötigt werden, um das Security Token zu erwerben.

2.3. WS-Federation

Im Rahmen von *Web Service Federation* (WS-Federation) soll betrachtet werden, wie Trust-Bündnisse konstruiert werden können. [IBMi02] folgend soll dies anhand eines Beispiels verdeutlicht werden: Alice, die bei Adventure456 arbeitet, möchte den Währungs-Web-Service von Business456 in Anspruch nehmen. Dieser bearbeitet jedoch lediglich Anfragen, denen ein von Business456 herausgegebenes Security Token beigefügt ist. Alice besitzt jedoch nur ein Security Token, mit Angaben zu ihrer Identität, welches von Adventure456 herausgegeben wurde. Alice kann den Währungs-WS also nur dann in Anspruch nehmen, wenn Business456 bereit ist, ein Sicherheitsbündnis mit Adventure456 einzugehen. Dazu sollen im Folgenden zwei Möglichkeiten aufgezeigt werden:
Der erste Ansatz geht davon aus, dass der Währungs-WS ausschließlich Security Token akzeptiert, die von Business456 herausgegeben wurden. Über die Policy des Web Service erfährt Alice, wo sie das benötigte Security Token erhalten kann. Alice legt dem Business456 Security Token Service ihr Adventure456 Security Token (inklusive Eigentumsnachweis) vor und erhält von ihm ein Business456 Security Token. Mit diesem kann sie nun eine Anfrage an

den Währungs-WS stellen. Abb. 2 veranschaulicht dieses Szenario.

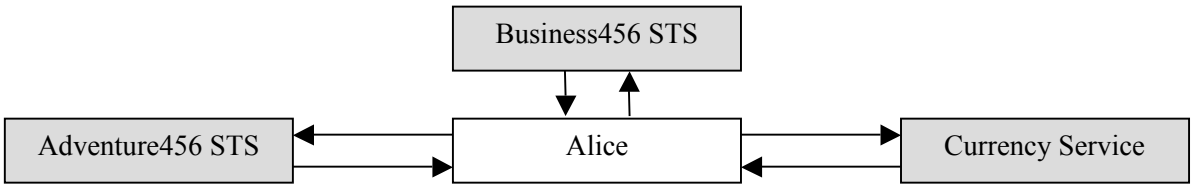

Abb. 2: Federation using security token exchange. Quelle: [IBMi02]

Im zweiten Ansatz wird das *Bündnis mittels einer Vertrauenskette* realisiert. Der Währungs–WS ist in diesem Fall so eingerichtet, dass er Anfragen mit allen möglichen Security Token akzeptiert, diese jedoch erst dann verarbeitet, wenn er im Tausch für das erhaltene Token ein Business456 Security Token erhalten hat. Dabei geht der Währungs-WS wie folgt vor: Die Anfrage des Dienstnutzers, sowie dessen Security Token, wird an den Business456 Security Token Service weitergeleitet, der das Token auswertet. Falls er es als gültig akzeptiert wird die Anfrage gebilligt und der Security Token Service übermittelt möglicherweise auch ein Business456 Security Token, welches Alice später ggf. wiederverwenden kann. Zu beachten ist in beiden Ansätzen, dass der Security Token Service von Business456 so eingerichtet ist, dass er den Identitätsnachweis, der von Adventure456 herausgegeben wurde, akzeptiert. Abb. 3 veranschaulicht dieses Szenario.

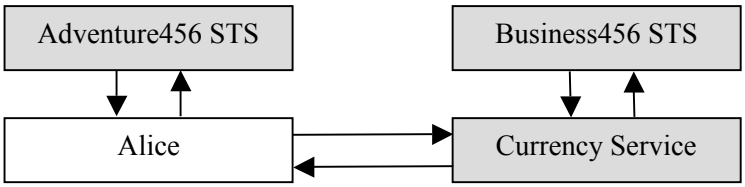

Abb. 3: Federation using trust chaining. Quelle: [IBMi02]

3. Reputation

3.1. Definitionen von Reputation in der Informatik und Klassifikation von Reputationsarten

Reputationssysteme kamen auf Grund ihres erfolgreichen Einsatzes, insbesondere im Bereich des E-Commerce, zu großem Ansehen. In wissenschaftlichen Berichten wurde herausgestellt, dass die Reputation eines Verkäufers entscheidenden Einfluss auf den Preis eines Gutes hat, der bei einer Online-Auktion erzielt werden kann. In Anlehnung an [HaMM02] sollen zunächst unterschiedliche Definitionen des Begriffes Reputation vorgestellt werden. Im Anschluss daran wird eine Klassifikation unterschiedlicher Reputationsbegriffe dargestellt.

In einer *allgemeinen Definition* des Begriffes lässt sich die Reputation eines Agenten als die Auffassung eines anderen Agenten über die Absichten und Normen dieses Agenten beschreiben. In der Wissenschaft existieren zahlreiche Verwendung für diesen Begriff. Beispielsweise erklären Ökonomen mit der Reputation irrationales Verhalten in der (ökonomischen) Spieltheorie, wohingegen er bei Biologen zur Erklärung der Kooperationsbereitschaft zwischen egoistisch denkenden Individuen Anwendung findet. Im Folgenden werden unterschiedliche Definitionen des Begriffes Reputation aus der Informatik dargestellt.

Die von Zacharia und Maes gegebene Definition der Reputation zielt auf *Bewertungen* ab, welche Agenten in Online-Communities von anderen Agenten erhalten. Das von ihnen entwickelte Sporas-System berechnet die Reputation eines Agenten als Mittelwert sämtlicher Bewertungen, die über diesen Agenten stattfanden. Ein ähnliches System findet z.B. im Online-Warenhaus Amazon Verwendung. Ein weiteres von ihnen entwickeltes System, Histos, berücksichtigt in der Bewertung der Reputation eines Agenten, wer eine Anfrage stellte und aus welcher Umgebung heraus.

Abdul-Rahman, et al., betrachten die Reputation als eine Form, *Kontrolle* in einem sozialen Kontext, in dem Trustwerte propagiert werden, *auszuüben*. Die Agenten kooperieren, um keine schlechte Reputation zu erhalten.

Sabater, et al., definieren Reputation als „opinion or view of one about something“. Dabei treffen sie drei Unterscheidungen des Begriffes: Die *individuelle Reputation* beschreibt, wie der Eindruck eines einzelnen Individuums von anderen beurteilt wird. Die *soziale Reputation* berücksichtigt bei der Bewertung des Individuums die soziale Gruppe, zu der dieses gehört. In der *ontologischen Definition* wird die Reputation in ihrem spezifischen Kontext betrachtet und soll somit die Vielfältigkeit des Begriffes berücksichtigen.

Eine auf Mui, et al., zurückgehende Definition des Begriffes Reputation verwendet *statistische Verfahren* zur Berechnung der Reputationswerte. Dabei erhält ein Agent, welcher Reputationswerte berechnet, die von den Nachbaragenten gespeicherten Werte für seine Auswertung. Die auf diese Weise erhaltenen Werte werden wiederum mit den Reputationswerten der Nachbarn, von denen die Werte stammen, gewichtet. Eine beispielhafte Veranschaulichung dieser Reputationsdefinition findet in Kapitel 3.3. an Hand des EigenTrust-Algorithmus statt.

Im Folgenden soll eine Klassifikation der unterschiedlichen Reputationsarten vorgenommen werden. Dazu wird von einem *kontextabhängigen Reputationsbegriff* ausgegangen. Anschaulich bedeutet Kontextabhängigkeit beispielsweise, dass die Reputation einer Person als Informatiker keinen Einfluss auf ihre Reputation als Koch hat. Die Klassifikation erfolgt in Anlehnung an [HaMM02].

Die erste Unterscheidung findet bezüglich des Personalisierungsgrades der Reputation statt. Dabei wird zwischen *globaler* und *personalisierter Reputation* unterschieden. Bei dem

Erforschen sozialer Netzwerke wird die Reputation als eine Größe betrachtet, die aus dem zugrunde liegenden Netzwerk abgeleitet wird. Dies bedeutet insbesondere, dass die Reputation eines Agenten für alle weiteren Agenten global sichtbar und identisch ist. Im Gegensatz dazu steht die personalisierte Reputation, bei der ein Agent unterschiedliche Reputationen aus den Perspektiven der anderen Agenten erhalten kann. Als Ursache können Ungewissheiten bezüglich der Umgebung identifiziert werden, die dafür verantwortlich sind, dass ein Agent im gleichen sozialen Kontext unterschiedlich bewertet wird.

Nach Abb. 4 wird auf oberster Stufe zwischen *Individual-* und *Gruppenreputation* unterschieden. In der Praxis eingesetzte Reputationssysteme (z.B. eBay und Amazon) beschränken sich dabei auf die individuelle Reputation, bei der ausschließlich einzelne Agenten bewertet werden. Die Gruppenreputation, aus der Perspektive eines Unternehmens, wurde von Ökonomen untersucht. Die Reputation eines Unternehmens wurde dabei als Durchschnitt der individuellen Reputationen aller Mitarbeiter modelliert.

In einem nächsten Schritt ist die Herleitung der individuellen Reputation zu betrachten. Diese kann entweder *direkt* oder *indirekt* hergeleitet werden. Direkte Reputation bezieht sich auf Erfahrungen, die ein Agent selbst mit einem anderen Agenten gemacht hat. Diese können sowohl beobachtet als auch selbst erfahren sein. Die indirekte Reputation basiert auf Informationen aus zweiter Hand, die ein Agent beispielsweise durch „Mundpropaganda“ erhalten hat.

Auf dritter Stufe wird die direkte Reputation unterschieden in Reputation, die auf Grundlage von *Interaktionen* abgeleitet wurde und solche, die durch *beobachtetes Verhalten* abgeleitet wurde. Das eBay-Reputationssystem bietet ein Beispiel für beide Arten der direkten Reputation. Nachdem eine Interaktion zwischen einem Käufer und einem Verkäufer stattgefunden hat, kann der Käufer den Verkäufer bewerten und somit direkt dessen Reputation im System beeinflussen. Käufer, die mit diesem Verkäufer noch nicht in Kontakt getreten sind, können die Bewertung der Agenten, die mit dem Verkäufer bereits Geschäfte abgeschlossen haben, abrufen und als beobachtete Reputation verwenden. In der hier verwendeten Terminologie ist entscheidend, dass die Begegnung zwischen dem bewertenden und dem bewerteten Agenten, welche Voraussetzung für die aus Interaktionen abgeleitete Reputation ist, bei der aus beobachtetem Verhalten abgeleiteten Reputation nicht stattgefunden hat.

Abschließend soll nun noch die indirekte Reputation untergliedert werden. Folgende Formen werden dabei unterschieden: zuvor abgeleitete, gruppenbasierte und propagierte Reputation. *Zuvor abgeleitete Reputationswerte* sind vergleichbar mit menschlichen Vorurteilen. In der Gesellschaft wird die Vertrauenswürdigkeit von Fremden häufig auf Grundlage von Vorurteilen eingeschätzt. Für Agenten gibt es unterschiedliche Ansätze die Reputation fremder Agenten mittels zuvor abgeleiteter Reputationswerte zu bestimmen. Mui, et al., schlagen dabei eine uniforme Verteilung für die Bewertung der Reputation fremder Agenten

vor. Zacharia und Maes weisen neuen Agenten den kleinst möglichen Reputationswert zu, so dass kein Ansporn besteht, einen Agenten, der mit seinem Reputationswert unter eine Startschwelle fällt, aufzugeben.

Reputationsmodelle für Gruppen können erweitert werden, um *(Vor)bewertungen sozialer Agenten in Gruppen* zu ermöglichen. Nach einer Studie von Tadelis wird vorgeschlagen, einen ökonomischen Agenten auf Grundlage des Unternehmens zu dem er gehört (vor)zubewerten. Dabei kann ein Agent von dem guten Ruf eines Unternehmens profitieren und umgekehrt.

Die *propagierte Reputation* erlaubt es einem Agenten, mittels Informationen, die er von anderen Agenten aus seiner Umgebung erhalten hat, fremde Agenten zu bewerten. Diese Form der Reputationsbewertung ist laut Abdul-Rahman und Hailes vergleichbar mit der menschlichen "Mund zu Mund Propaganda". Reputationsinformationen können dabei von Agent zu Agent übertragen werden.

3.2. Reputation verdeutlicht am eBay-Reputationssystem

Das Internet bietet seinen Benutzern zahlreiche Möglichkeiten der Interaktion mit Fremden. Bedingt durch die Anonymität des Mediums ergeben sich insbesondere im Hinblick auf Geschäftsbeziehungen erhöhte Risiken für die Benutzer. Reputationssysteme sollen helfen Vertrauensbeziehungen z.B. zwischen Geschäftspartnern aufzubauen und das Risiko betrügerischer Geschäfte zu minimieren. Zur Veranschaulichung soll das eBay-Reputationssystem in Anlehnung an [FKR+00] näher betrachtet werden.

Reputationssysteme sammeln Informationen (Feedback) über das vergangene Verhalten ihrer Teilnehmer, stellen diese zusammen und verbreiten sie. Da wenige der Anbieter und Konsumenten, welche Bewertungen vornehmen, sich gegenseitig kennen, helfen diese Systeme den Teilnehmern zu entscheiden, wem sie Vertrauen entgegenbringen. Darüber hinaus schrecken sie unehrliche Geschäftsleute ab, an diesen Systemen teilzunehmen.

Dass Reputationssysteme geeignet sind erfolgreiche Geschäftsabschlüsse zwischen gegenseitig unbekannten Geschäftspartnern zu ermöglichen kann anhand des Internet-Auktionshauses eBay verdeutlicht werden. Obwohl das Auktionshaus selbst keinerlei Garantie für seine Auktionen übernimmt und somit das Risiko allein bei den Käufern und Verkäufern liegt, sind dennoch stets mehr als vier Millionen Auktionen gleichzeitig offen. Dabei liegt die Anzahl erfolgreich abgeschlossener Transaktionen für einen Markt, der betrügerische Transaktionen auf einfache Weise ermöglicht, erstaunlich hoch.

Beim eBay-Reputationssystem handelt es sich um ein *Feedback Forum*. Nachdem eine Transaktion abgeschlossen wurde haben Käufer und Verkäufer die Möglichkeit sich

gegenseitig zu bewerten. Dabei bewerten sie zufriedenstellende Transaktionen mit 1, neutrale mit 0 und nicht zufriedenstellende Transaktionen mit –1. Darüber hinaus können Kommentare im Forum hinterlassen werden (beispielsweise "Es ist sehr empfehlenswert, mit dieser Person Geschäfte abzuschließen."). Die Feedback-Punkte sind dabei direkt mit dem Namen des Teilnehmers (möglicherweise ein Pseudonym) sichtbar verbunden.

Um die Frage zu beantworten, weshalb solche Reputationssysteme geeignet sind um Vertrauen zwischen Fremden aufzubauen soll zunächst betrachtet werden, wie Vertrauen in dauerhaften Geschäftsbeziehungen aufgebaut wird, in denen die Geschäftspartner gegenseitig bekannt sind. Der erste Aspekt zur Etablierung von Vertrauen bei der Interaktion mit einem Geschäftspartner betrifft dessen Fähigkeiten und Absichten. Auf Grund vergangener Interaktionen kann beurteilt werden, in welchen Situationen man sich auf den Geschäftspartner verlassen kann. Als zweiter Aspekt ist die Erwartung von Vergeltung in der Zukunft als Ansporn zu gutem Verhalten in der Gegenwart zu betrachten.

Diese beiden Voraussetzungen sind bei Geschäftsbeziehungen zwischen Fremden im Internet nicht gegeben, es kann meist weder auf Erfahrungen aus Interaktionen aus der Vergangenheit zurückgegriffen werden, noch sind zukünftige Interaktionen zu erwarten. Da kein Informationsnetzwerk zugrunde liegt, welches gutes Verhalten belohnt und schlechtes bestraft, steht auch der Name der Geschäftspartner nicht auf dem Spiel. Für betrügerische Geschäftsabschlüsse sind also keine negativen Konsequenzen zu erwarten, so dass ein Ansporn zum Betrug geschaffen wird.

Reputationssysteme versuchen Auswirkungen vergangener Transaktionen Relevanz für die Zukunft zu verleihen. Zwar besteht meist keine Verbindung zwischen den Teilnehmern an Reputationssystemen untereinander, von Bedeutung ist jedoch ihre große Anzahl. Dabei kann die große Anzahl an Informationen über einen Geschäftspartner (dieser wurde möglicherweise von sehr vielen Teilnehmern bewertet) die niedrige Qualität der Information (Bewertung nur mittels Auswahl aus drei möglichen Werten und ggf. Kommentar) kompensieren. Im Beispiel des Auktionshauses eBay kann dies folgendes bedeuten: Zahlreiche Käufer interagieren mit dem gleichen Verkäufer. Wenn diese ihre Meinung über den Verkäufer im Feedback Forum zur Verfügung stellen, so kann eine aussagekräftige Historie über diesen angelegt werden, auf deren Grundlage andere Käufer, die zuvor noch nicht mit dem Verkäufer interagiert haben, eine Entscheidung über einen Geschäftsabschluss herbeiführen können. Wenn die Käufer die Historie eines Verkäufers als Grundlage für Kaufentscheidungen nutzen, dann wirkt sich die Reputation eines Verkäufers direkt auf dessen zukünftige Verkäufe aus, so dass dieser bemüht sein wird, so viele positive Bewertungen wie möglich zu erhalten.

An dieser Stelle soll die Frage betrachtet werden, wie Interaktionen mit Geschäftspartnern mit niedrigen Reputationswerten (z.B. neu angemeldete Teilnehmer am Reputationssystem) zu erklären sind. Nach der operationalen Definition des Begriffes Trust, welche auf das

statistisch bzw. deterministisch messbare Risiko abzielt, dürften Geschäftsbeziehungen zwischen Geschäftspartnern, von denen mindestens einer einen niedrigen Reputationswert aufweist, auf Grund des erhöhten Risikos einer betrügerischen Transaktion nicht zu Stande kommen. Tatsächlich gibt es jedoch Transaktionen dieser Art. Das „irrationale“ Verhalten eines Geschäftspartners, mit einem Kunden bzw. Anbieter mit niedrigen Reputationswerten Geschäfte abzuschließen lässt sich mittels der Definition des Begriffes Trust als interner Zustand erklären. Der Kooperationswille des Geschäftspartners wird dabei als Erklärung für solche Transaktionen herangezogen. Dieser kann beim Käufer beispielsweise durch einen günstigen Preis oder durch ein besonderes Gut beeinflusst werden, so dass er trotz erhöhtem Risiko bereit ist dem Geschäftsabschluss zuzustimmen.

Um funktionsfähig zu arbeiten werden also drei Eigenschaften eines Reputationssystems minimal vorausgesetzt:

- die Objekte des Systems existieren dauerhaft, es wird erwartet, dass sie an zukünftigen Interaktionen teilnehmen werden
- das Feedback über Interaktionen wird gesammelt und verbreitet; diese Information muss in der Zukunft sichtbar sein
- das Feedback aus der Vergangenheit beeinflusst Kaufentscheidungen in der Gegenwart bzw. Zukunft

Reputationssysteme sind vielversprechend, um die Risiken von Interaktionen zwischen gegenseitig unbekannten (Geschäfts-)Partnern zu reduzieren. Es verbleiben jedoch Probleme, die weitere wissenschaftliche Arbeit und kommerzielle Entwicklung an diesen Systemen erfordern. Diese werden im Folgenden, anhand der drei Phasen, die ein Reputationssystem kennzeichnen, erläutert:

Zunächst muss ein *Feedback* über die Interaktion von den Interaktionspartnern *erhalten* werden. Damit sind wiederum drei Probleme verbunden. Als erstes Problem kann die häufig *fehlende Motivation zum Ausfüllen von Formularen*, nach dem erfolgreichen Abschluss einer Interaktion, genannt werden. Anreize in Form von Bezahlungen für sorgfältig vorgenommene Bewertungen sind hier denkbar. Das zweite Problem besteht in der *Schwierigkeit* den Interaktionspartnern *negatives Feedback zu entlocken*. Anhand des Auktionshauses eBay kann aufgezeigt werden, dass es in der Praxis üblich ist, nur sehr schlechte Geschäftsabschlüsse negativ zu bewerten. Als Grund wird z.B. die Angst vor einer schlechten Bewertung in Retour angeführt. Unehrliche Bewertungen stellen das dritte Problem dar. So ist es denkbar, dass Teilnehmer am Reputationssystem durch Erpressung gezwungen werden unehrliche Bewertungen abzugeben. Aber auch Gruppen, deren Mitglieder sich untereinander positiv bewerten, und somit ihre Reputation künstlich erhöhen, stellen ein Problem dar.

Nachdem man *Feedback* von den Interaktionspartnern erhalten hat, muss dieses in einem zweiten Schritt *zusammengefasst* werden. Die Darstellung soll dabei möglichst so erfolgen, dass sie eine Entscheidungsgrundlage dafür bietet, wem man Vertrauen entgegen bringen

kann. Bei eBay werden lediglich positive und negative Bewertungen aufsummiert, andere Systeme berechnen Mittelwerte. Eine *Differenzierung* zwischen Bewertungen von Teilnehmern mit hoher Reputation und solchen mit niedriger Reputation wird allerdings nicht vorgenommen. Auch der *Wert des Gegenstandes* einer Transaktion findet in diesen Reputationssystemen keine Berücksichtigung. In zukünftigen Reputationssystemen könnte man an diesen Schwachpunkten ansetzen, um aussagekräftigere Reputationswerte zu erhalten.
Der dritte Schritt besteht in der *Verbreitung der Information.* Diese ist wiederum mit zwei Schwierigkeiten verbunden. Die erste besteht in der *Möglichkeit der Namensänderung*. Teilnehmer wählen einen Namen, wenn sie sich bei einem Reputationssystem registrieren. Wenn sie sich später unter einem neuen Namen registrieren, wird das Feedback, das sie in der Vergangenheit erhalten haben, bedeutungslos. Durchgeführte Analysen in der Spieltheorie ergaben, dass die Möglichkeit der Namensänderung die Effektivität von Reputationssystemen reduziert. Lösungsansätze bestehen darin, eine Anmeldegebühr zu erheben, oder bei Neuanmeldung niedrige Reputationswerte zu vergeben, so dass z.B. nur geringere Preise für Waren erzielt werden können. Auch kann das Anfordern mehrerer Pseudonyme für eine Person unterbunden werden. Als zweite Schwierigkeit wird die *mangelnde Portabilität* zwischen den Reputationssystemen betrachtet. Amazon.com erlaubte es seinen Benutzern ursprünglich ihre eBay-Reputationswerte zu importieren, dies wurde jedoch von eBay verboten. Die Konsequenz ist, dass die Reichweite der Reputationswerte sich jeweils auf ein System beschränken und somit die Effektivität des Feedbacks reduziert wird. Zur Lösung dieses Problems werden universelle Reputationssysteme entwickelt, für welche die nötige gesellschaftliche Akzeptanz jedoch noch zu entwickeln ist.

3.3. Trust auf Grundlage von Reputation: Der EigenTrust-Algorithmus

Den Vorteilen der Peer-to-Peer (P2P) Filesharing-Netzwerke (wie z.B. verbesserte Robustheit, Erweiterbarkeit und Vielfältigkeit der verfügbaren Daten) stehen im Hinblick auf Sicherheit einige Nachteile entgegen. Bedingt durch die Anonymität der Peers in diesen Netzwerken ist es nicht möglich, Inhalte den einzelnen Peers zuzuordnen, die sie zur Verfügung stellen. Dies führte in der Vergangenheit dazu, dass böswillige Benutzer unbrauchbare Dateien, aber auch Viren, wie beispielsweise den VBS.Gnutella Wurm, in diesen Netzwerken verteilten.
Für Agenten in diesen Netzwerken stellt sich die Frage, wieviel Vertrauen (Trust) sie anderen Agenten entgegenbringen können. Diese Einschätzung wird häufig auf Grundlage der Reputation der Agenten, mit denen die Interaktion stattfinden soll, vorgenommen. Im Folgenden ist insbesondere die Individualreputation aus der in Kapitel 3.2. vorgestellten

Reputationsklassifikation relevant, welche das direkte oder indirekte Wissen über frühere Interaktionen, mit dem Agenten, mit dem die Interaktion stattfinden soll, zur Bewertung heranzieht.

Das Problem des Trust Management in dezentralen Informationssystemen untergliedert sich laut [AbDe01] dabei in die folgenden drei Unterprobleme:

- Bestimmung des globalen Trust-Modells, welches beschreibt, ob ein Agent vertrauenswürdig ist (z.B. auf Grundlage von statistischen Methoden)
- Definition eines lokalen Algorithmus zur Bestimmung von Trust; dieser muss die Vertrauenswürdigkeit und Erreichbarkeit von Agenten im Netzwerk berücksichtigen und eine gute Annäherung an das globale Trust-Modell bieten
- Daten- und Kommunikationsmanagement: um eine erweiterbare Implementierung zu erhalten sollen die Ressourcen, die jeder Agent benötigt, in der Anzahl der Agenten *n*, möglichst in O(log *n*) steigen

Im Folgenden soll anhand des EigenTrust-Algorithmus aufgezeigt werden, wie Trust auf Grundlage von Reputation etabliert werden kann. Um zuverlässige Informationen über die Qualität eines Peers, von dem ein Benutzer Dateien lädt, zu erhalten und solche Peers, die unbrauchbare Dateien zur Verfügung stellen zu identifizieren, kann der in Anlehnung an [GaKS03] beschriebene Algorithmus eingesetzt werden. Das globale Trust-Modell ist hier wie folgt definiert: Auf Grundlage eines verteilt berechneten, globalen Trust-Wertes für jeden im Netzwerk befindlichen Peer i, der die Erfahrung aller übrigen Peers mit i widerspiegelt, sollen böswillige Peers identifiziert und aus dem Netzwerk isoliert werden.

Der Algorithmus arbeitet wie folgt: Nachdem Peer i eine Datei von Peer j geladen hat, bewertet Peer i die Transaktion. Dabei gilt $tr_{i,j} = 1$, falls Peer i den Download positiv und $tr_{ij} = -1$, falls Peer i den Download als negativ (im Sinne von nicht zufriedenstellend) bewertet. Ein *lokaler Trust-Wert* des Peers i für Peer j kann dann wie folgt definiert werden: $s_{ij} = \sum tr_{ij}$.

Die Herausforderung besteht nun darin, die lokalen Trust-Werte für Peer j zu einem globalen Trust-Wert zu aggregieren. Dabei sollen möglichst alle lokalen Werte in die Berechnung einbezogen werden, das dazu nötige Nachrichtenaufkommen soll jedoch das Neztwerk nicht zu stark belasten.

Um die lokalen Trust-Werte zusammenzufassen ist es nötig zuvor eine *Normalisierung* durchzuführen. Damit soll verhindert werden, dass böswillige Peers anderen böswilligen Peers hohe und gutwilligen Peers niedrige Trust-Werte zuweisen. Der normalisierte Trust-Wert c_{ij} berechnet sich dabei wie folgt: $c_{ij} = \frac{\max(s_{ij},0)}{\sum_j \max(s_{i,j},0)}$. Somit liegen alle normalisierten Werte zwischen null und eins. Für den Fall, dass $\sum_j \max(s_{i,j},0) = 0$ gilt, ist c_{ij} nicht definiert.

Zwei Nachteile sind beim normalisierten Trust-Wert zu beachten: Erstens handelt es sich bei

den Werten für c_{ij} um relative Wert, die nicht absolut interpretiert werden können. Für $c_{ij} = c_{ik}$ lässt sich somit nur feststellen, dass die Peers j und k von i gleich bewertet werden, ob gut oder schlecht kann dabei nicht gesagt werden. Zweitens wird nicht unterschieden, ob ein Peer i wenig oder keine Erfahrung mit Peer j gemacht hat. Trotz dieser Nachteile können mit dem Algorithmus gute Ergebnisse erzielt werden.

Um nun die normalisierten Trust-Werte zu *aggregieren* befragt (wie in einer verteileten Umgebung üblich) Peer i seine Nachbarn nach ihrer „Meinung" über andere Peers. Diese Meinung wird mit der Einschätzung von Peer i über den Nachbarn gewichtet: $t_{ik} = \sum_j c_{ij} c_{jk}$.

Diese Darstellung soll nun in Matrixschreibweise überführt werden. Sei C die Matrix $[c_{ij}]$ und t_i der Vektor mit den Werten t_{ik}, so gilt: $t_i = C^T c_i$, mit $\sum_j t_{ij} = 1$, wie gewünscht. Die Übersicht eines Peers i über das Netzwerk ist zwar auf diese Weise größer geworden als die vorherige, jedoch handelt es sich immernoch nur um die Sicht von i und dessen Nachbarn. Es können nun mittels $t = (C^T)^2 c_i$ die Nachbarn der Nachbarn einbezogen werden. Nach n Iterationen (für n groß) könnte auf diese Weise ein Überblick über das gesamte Netzwerk erhalten werden ($t = (C^T)^n c_i$), falls C nicht reduzibel und nicht periodisch ist. Für n groß konvergieren die Trust-Vektoren t_i für alle Peers i gegen den gleichen Vektor, nämlich den Eigenvektor von C. Somit ist t ein globaler Trust-Vektor, dessen Elemente $\square_j$ das Vertrauen des gesamten Systems in Peer j quantifizieren.

Eine mögliche *probabilistische Interpretation* dieser Methode soll im Folgenden dargestellt werden. Ein Agent, der auf der Suche nach Peers mit hohen Reputationswerten ist, durchläuft das Netzwerk nach folgender Regel: Bei jedem Peer i geht der Agent mit Wahrscheinlichkeit c_{ij} als nächstes zu Peer j. Nachdem der Agent das Netzwerk eine Weile auf diese Weise durchlaufen hat, ist die Wahrscheinlichkeit, dass er zu einem Peer mit guter Reputation gelangt ist größer als die Wahrscheinlichkeit, dass er zu einem Peer mit schlechter Reputation gelangt ist. Die stationäre Verteilung der Markov-Kette, die durch die normalisierten, lokalen Trust-Werte der Matrix C repräsentiert wird, entsprechen dem globalen Trust-Vektor t.

Abschließend soll nun eine vereinfachte Version des EigenTrust Algorithmus vorgestellt werden, welche den Aspekt der Verteilung in einem P2P-Netzwerk zunächst nicht berücksichtigt. Dazu ist davon auszugehen, dass ein zentraler Server alle Werte c_{ij} kennt und die Berechnung durchführt. Hauptsächlich geht es um die Berechnung von $t = (C^T)^n e$, für n groß. Dabei ist e ein m-stelliger Vektor, der Form $e_i = 1/m$ (gleichförmige Verteilung über alle m Peers). Auf diese Weise ergibt sich folgender Algorithmus:

$t^{(o)} = e;$
repeat
$t^{(k+1)} = C^T t^{(k)};$
$\delta = \left\| t^{(k+1)} - t^{(k)} \right\|;$
until($\delta < \varepsilon$)

Abb.2: Einfacher, nicht verteilter EigenTrust-Algorithmus
Quelle: [GaKS03]

In einer verteilten Umgebung müssen *Aspekte der Sicherheit* berücksichtigt werden. Im oben beschriebenen Algorithmus berechnet Peer i seinen eigenen Trust-Wert t_i und gibt diesen auf Anfrage weiter. Böswillige Peers können dabei leicht falsche Trust-Werte weitergeben und somit das System schädigen. Zwei Verfahren sollen dieses Problem lösen. Erstens sollen Peers nicht ihre eigenen Trust-Werte berechnen und speichern. Diese Aufgabe wird von anderen Peers im Netzwerk übernommen. Zweitens wird der Trust-Wert eines Peers von mehr als einem Peer im Netzwerk berechnet, da es im Interesse böswilliger Peers liegt falsche Trust-Werte für andere Peers zurückzugeben. Einem Peer wird dann der Trust-Wert zugewiesen, der mehrheitlich ermittelt wurde.
Abschließend lässt sich feststellen, dass der EigenTrust-Algorithmus geeignet ist, den Einfluss böswilliger Peers in einem P2P-Netzwerk zu minimieren. Unter Berücksichtigung der Historie des gesamten Systems wird ein globaler Trust-Wert für jeden im Netzwerk befindlichen Peer berechnet. Diese Berechnungen sind skalierbar und können verteilt realisiert werden. Die Anzahl inauthentischer Datei-Downloads kann mit Hilfe des Algorithmus in einer Vielzahl von Threat-Szenarien erheblich reduziert werden.

4. Privacy

Der Schutz persönlicher Daten (im Englischen Privacy) spielt für Internetbenutzer eine zunehmend größere Rolle. Sie sind besorgt, welche persönlichen Informationen sie preisgeben, wenn sie online gehen und wer diese Informationen schließlich erhält. Nicht selten hört man von Unternehmen, die Einkünfte aus persönlichen Informationen, welche sie auf ihren Internetseiten gesammelt haben, erzielen. So werden Informationen, die Internetbenutzer zur Verfügung stellen um sich bei einem Dienst zu registrieren häufig zum Telemarketing gebraucht oder an andere Unternehmen verkauft.
Persönliche Informationen werden auf Webseiten mit Hilfe von *Cookies* gesammelt. Für den Internetbenutzer ergibt sich dabei das Problem, dass er möglicherweise Informationen, die er geheimhalten möchte preisgibt, wenn er Internetseiten das Setzen von Cookies erlaubt.

Verbietet er das Setzen von Cookies jedoch, so stehen ihm Funktionalitäten wie Online-Banking und Online-Shopping bei einigen Webseiten nicht zur Verfügung.

Anhand von *Privacy Policies*, die Dienstanbieter im Internet zur Verfügung stellen, kann ein Dienstnutzer erfahren, wie ein Dienstanbieter mit seinen persönlichen Informationen umgeht. Jedoch sind diese Policies, die meist in natürlicher Sprache formuliert sind, für Dienstnutzer sehr zeitaufwendig zu lesen und schwierig zu verstehen. Es ist für Dienstnutzer kompliziert herauszufinden, wie sie die Verwendung ihrer persönlichen Informationen unterbinden können.

Der Umfang und die Unverständlichkeit der Dokumente stehen im Konflikt zu dem erhöhten Informationsbedarf der Dienstnutzer über die Privacy Policies der Dienstanbieter. Der P3P-Standard bietet eine Lösung dieses Problems, indem er einen Standard anbietet, der die Verarbeitung der Privacy Policies durch den Computer ermöglicht, sowie ein Protokoll, welches es Web-Browsern und anderen Agenten möglich macht, Privacy Policies automatisch zu lesen und zu verarbeiten. Einige der verfügbaren Tools können die Privacy Policy der Dienstanbieter mit den Privacy-Bedüfnissen der Dienstnutzer vergleichen und somit die Entscheidung unterstützen, ob ein Benutzer Daten mit einem Dienst austauschen möchte oder nicht.

Im Gegensatz zu Tools, die ausschließlich der Anonymisierung von Benutzerndaten dienen ist herauszustllen, dass das Ziel des P3P-Ansatzes nicht darin besteht keinerlei persönliche Informationen bereitzustellen. Statt dessen soll eine verbesserte *Entscheidungsgrundlage* geschaffen werden, die es dem Benutzer ermöglicht zu entscheiden, wann und mit welchem Dienst er persönliche Informationen austauschen möchte. Dieser Ansatz kann jedoch ggf. mit dem Einsatz von Tools zur Anonymisierung von Benutzerdaten kombiniert werden, wenn ein Benutzer entscheidet, dass er keine persönlichen Informationen preisgeben möchte.

Nachfolgend soll die arbeitsweise von P3P in Anlehnung an [Fait02] näher betrachtet werden. Bei einer P3P Policy handelt es sich im Wesentlichen um einen Antwortkatalog zu einer Vielzahl von Multiple-Choice-Fragen, welche beschreiben, wie Dienstanbieter mit den Informationen, die sie von Dienstnutzern erhalten, im Hinblick auf Datenschutz umgehen. Der Vorteil bei fest vorgegebenen Fragen besteht darin, dass die Antworten durch den Computer automatisch verarbeitet werden können. Jedoch sind die in der Policy enthaltenen Informationen im Vergleich zu Policies, die in natürlicher Sprache formuliert sind, weniger detailliert.

Wie findet nun eine Dienstanfrage unter Verwendung von P3P Policies statt? Der Agent des Benutzers (z.B. sein Web-Browser) sendet eine Anfrage nach der Referenzdatei zur Policy des Dienstanbieters, dessen Dienst er nutzen möchte. Die Referenzdatei enthält Informationen darüber, wo die Policy für entweder den gesamten Dienst oder einzelne Policies für Teildienste abgerufen werden können. Der Agent des Benutzers lädt die geeignete Policy,

wertet diese aus und führt die Verarbeitung der Dienstanfrage entsprechend der Datenschutzbedürfnisse des Benutzers fort.

Die Ergebnisse der Verarbeitung der Policy werden dem Benutzer üblicherweise innerhalb des Agenten angezeigt. Dazu existieren meist Symbole, die die Privacy Policy des Dienstanbieters zusammenfassen, oder darauf hinweisen, dass ein Zertifikat existiert, welches belegt, dass der Dienstanbieter seine veröffentlichte Privacy Policy bzw. allgemeine Privacy-Standards erfüllt. Häufig wird es dem Benutzer auch ermöglicht, durch einfaches klicken eines Buttons, die in natürlicher Sprache geschriebene Policy zu laden und anzuzeigen, ohne dass der Benutzer selbst im Netz danach suchen muss.

Anhand des Microsoft Internet Explorer 6 (IE6) soll beispielhaft die Funktionalität verfügbarer Agenten verdeutlicht werden. Eine Besonderheit des Browsers im Hinblick auf P3P besteht darin, dass er automatisch kompakte P3P Policies von Webseiten überprüft, welche Cookies setzen. Der Benutzer kann diesen Agenten so konfigurieren, dass Cookies, die keine kompakte Policy besitzen, oder deren Policy nicht den Privacy-Anforderungen der Benutzer entsprechen, herausgefiltert werden. Auf diese Weise blockierte Cookies werden dem Benutzer mittels eines „Auges“ am rechten unteren Fensterrand des Browsers angezeigt. Wählt der Benutzer die Option „Privacy Report“, so läd IE6 automatisch die P3P Privacy Policy der entsprechenden Webseite, generiert daraus eine Version in natürlicher Sprache und zeigt diese dem Benutzer an.

Abschließend sollen Gründe betrachtet werden, die Dienstanbieter motivieren P3P einzusetzten. Nach [Fait02] sind insbesondere folgende Gründe relevant:

- Dienstanbieter setzen P3P ein, um ihren Kunden zu verdeutlichen, dass sie deren Privacy-Bedürfnisse respektieren. P3P ermöglicht es den Kunden, ihre Daten aus Marketing- und Mailinglisten zu entfernen. Unternehmen, die mit der Einhaltung von Privacy-Richtlinien werben, erhoffen sich ein Aufwertung der eigenen Marke.
- Dienstanbieter erwarten, dass P3P in Zukunft ein Standard sein wird, dem Kunden Bedeutung beimessen werden. Wenn Kunden die Möglichkeit haben werden, bei zahlreichen Dienstanbietern einen Privacy Report einer Webseite anzufordern oder ein Symbol auf dem Bildschirm zu sehen, welches die Einhaltung des P3P-Standards anzeigt, so befürchten die Unternehmen, dass Kunden misstrauisch gegenüber solchen Anbietern sein werden, die diesen Standard nicht erfüllen.
- Webseiten, die den P3P-Standard nicht erfüllen können auf neuen Browsern teilweise nicht korrekt angezeigt werden. Beispielsweise überprüft IE6 direkt ob kompakte Policies für Cookies von Drittanbietern existieren. Ist dies nicht der Fall, so werden diese blockiert. Gezielte Werbung, Seitenzähler, etc. funktionieren dann auf Seiten, die den P3P-Standard nicht erfüllen nicht.

Auch im Bereich von Web Services gibt es Bemühungen den Privacy-Bedürfnissen von Dienstnutzern und Dienstanbietern gerecht zu werden. Ein Standard existiert hier jedoch noch

nicht. Anhand eines Beispiels soll aufgezeigt werden, wie Privacy für Dienstnutzer eines Web Services realisiert werden kann. Ein Agent möchte einen Kalender-Web_Service nutzen. Der Agent hat zuvor seine Privacy-Bedürfnisse in einer Service Policy bekannt gegeben. Der Kalender-WS besitzt Privacy-Richtlinien, in denen er erklärt, wie er mit den Daten, welche er von den Dienstnutzern erhält, im Bezug auf Datenschutz umgeht. Wenn nun der Agent den Dienst beim Kalender-WS anfragt, so vergleicht dieser die Privacy-Bedürfnisse des Agenten mit seinen Richtlinien und trifft auf dieser Grundlage eine Entscheidung darüber, ob der Agent seinen Dienst nutzen darf, oder nicht. In Abb 3. wird dieses Szenario veranschaulicht.

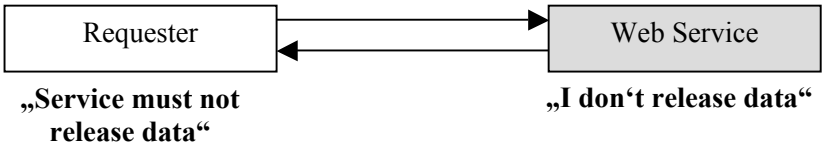

Abb. 3: Privacy statements in service policies. Quelle: [IBMi02]

5. Konklusion

Aktuelle Bemühungen von Experten zur Gewährleistung von Sicherheit in Netzwerken konzentrieren sich auf die technologischen Herausforderungen, wie beispielsweise das Entwickeln von Trust-Mechanismen (diese sind u.a. Grundlage für das von IBM und Microsoft entwickelte WS-Trust-Modell, welches in Kapitel 2.2. vorgestellte wurde) und das Entwerfen von Policies. Zwar sind diese Bemühungen zur Etablierung von Trust von zentraler Bedeutung, nach [Camp02] könnten jedoch bessere Erfolge erzielt werden, wenn das (teilweise irrationale) Verhalten von sozialen Agenten (Individuen und Organisationen) in vernetzten Informationssystemen mehr Beachtung finden würde. Ein systematisches Verständnis, wie soziale Agenten an Trust-Beziehungen teilnehmen bzw. zur Etablierung von Trust beitragen, sollte zukünftig beim Design solcher Informationssysteme ebenso beachtet werden, wie das zugrunde liegende Netzwerk, die Protokolle und Policies. Innerhalb der operationalen Definition des Begriffes Trust wurde beispielhaft in diesem Zusammenhang das Vertrauen auf Grundlage von Eigeninteressen vorgestellt.

Zum Aufbau kurzzeitiger Vertrauensbeziehungen haben sich Reputationssysteme als wirksam erwiesen, welche Vertrauen (Trust) auf Grundlage der Individualreputation eines Agenten etablieren. Die sich ergebenen theoretischen und praktischen Probleme, welche in Kapitel 3.2.1 thematisiert wurden (beim Erhalten, Aggregieren und Verbreiten von Feedback) beeinflussen die Performanz dieser Systeme nicht wesentlich. Das Vertrauen, welches Benutzer diesen Reputationssystemen entgegenbringen, ergibt sich einerseits aus der Vielzahl der Benutzer und andererseits durch die effektive Arbeitsweise dieser Systeme über einen langen Zeitraum. Aktuelle Bemühungen konzentrieren sich u.a. darauf die Reichweite von

Reputationswerten einzelner Reputationssysteme und somit auch deren Bedeutung zu erhöhen. Zu diesem Zweck sollen universelle Reputationssysteme wie virtualfeedback.com entwickelt werden, welche Bewertungen über mehrere Reputationssysteme zulassen.

Ein Möglichkeit Privacy für Dienstnutzer zu realisieren stellt der in Kapitel 4 vorgestellt P3P-Standard dar. Er bietet eine Implementierungsgrundlage für Benutzeragenten, die Dienstnutzer bei der Entscheidung unterstützen sollen, welche persönlichen Daten sie einem Dienst preisgeben bzw. vor ihm geheimhalten möchten. Um ein am Menschen orientiertes Trust-Konzept in ein vernetztes Informationssystem zu integrieren soll laut [Camp02] der Datenschutz (Privacy) zukünftig bereits bei der Implementierung solcher Systeme (und nicht erst im Nachhinein) stärker berücksichtigt werden.

6. Literatur

AbDe01 Aberer, K.; Despotovic, Z.: Managing Trust in a Peer-2-Peer Information System, *Proceedings of the Ninth International Conference on Information and Knowledge Management, CIKM, Atlanta, Georgia, USA, 5.–10. November 2001,* Seite 310

Camp02 Camp, L. J.: Designing for Trust, *Workshop on Deception, Fraud and Trust in Agent Societies, AAMAS 2002 International Workshop, Bologna, Italy, 15.07.2002*, Seite 15

FKR+00 Friedman, E.; Kuwabara, K.; Resnick, P.; Zeckhauser, R.: Reputation Systems: Facilitating Trust in Internet Interactions, *Communications of the ACM, CACM, Volume 43, Number 12, December 2000*, Seite 45

GaKS03 Garcia-Molina, H.; Kamvar, S. D.; Schlosser, M. T.: The EigenTrust Algorithm for Reputation Management in P2P Networks, *Proceedings of the Twelfth International World Wide Web Conference, WWW2003, Budapest, Hungary, 20.-24. May 2003*

GrSl03 Grandison, T.; Sloman, M.: Trust Management Tools for Internet Applications, *First International Conference, iTrust 2003, Heraklion, Crete, Greece, May 2003*, Seite 91

HaMM02 Halberstadt, A.; Mohtashemi, M.; Mui, L.: Evaluating Reputation in Multi-agents Systems, *Workshop on Deception, Fraund and Trust in Agent Societies, AAMAS 2002 International Workshop, Bologna, Italy, 15.07.2002*, Seite 123

IBMi02 o.V.: *Security in a Web Services World: A Proposed Architecture and Roadmap*, IBM Corporation and Microsoft Corporation, 2002 Elektronisch verfügbar unter: http://www-106.ibm.com/developerworks/ library/ws-secmap/

Fait02 Faith Cranor, L.: *Web Privacy with P3P*, O'Reilly & Associates, 2002

7. Anhang

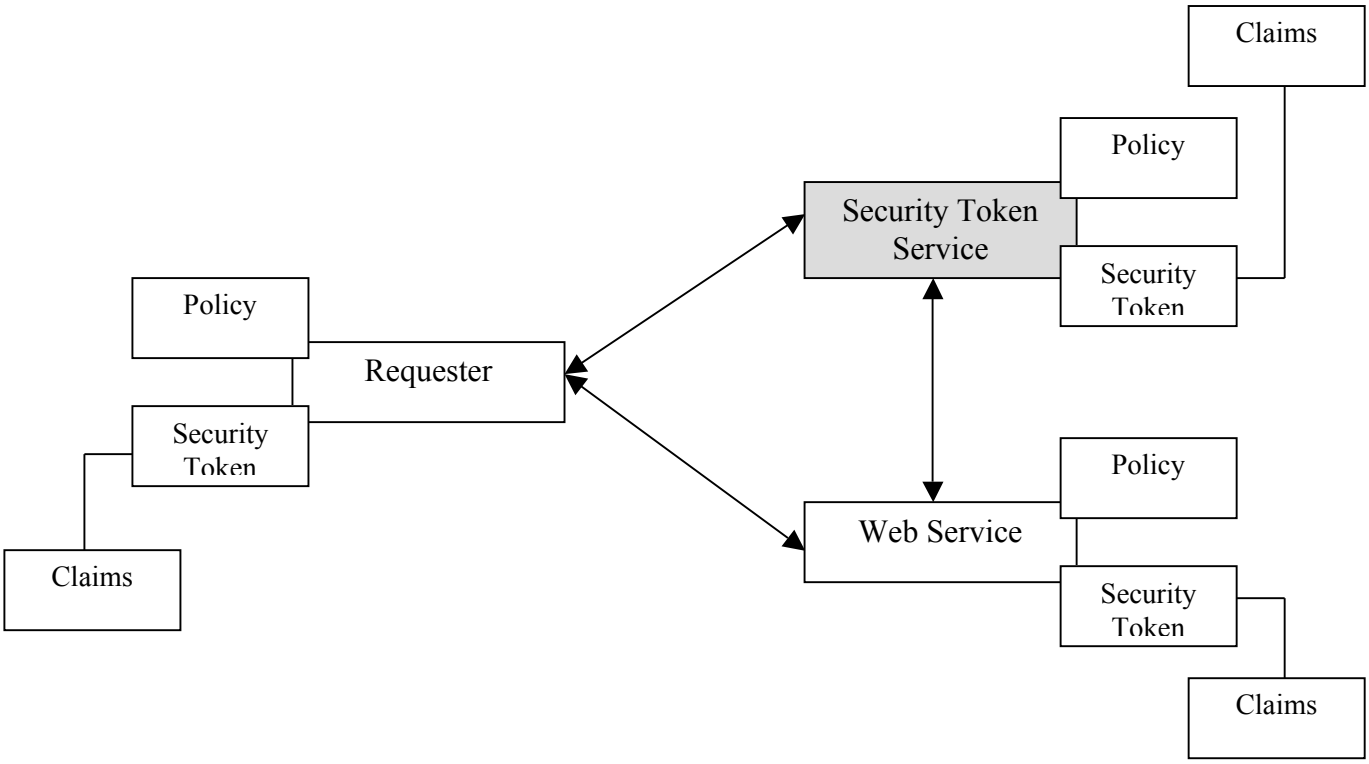

Abb. 1: Security Token Service Model. Quelle: [IBMi02]

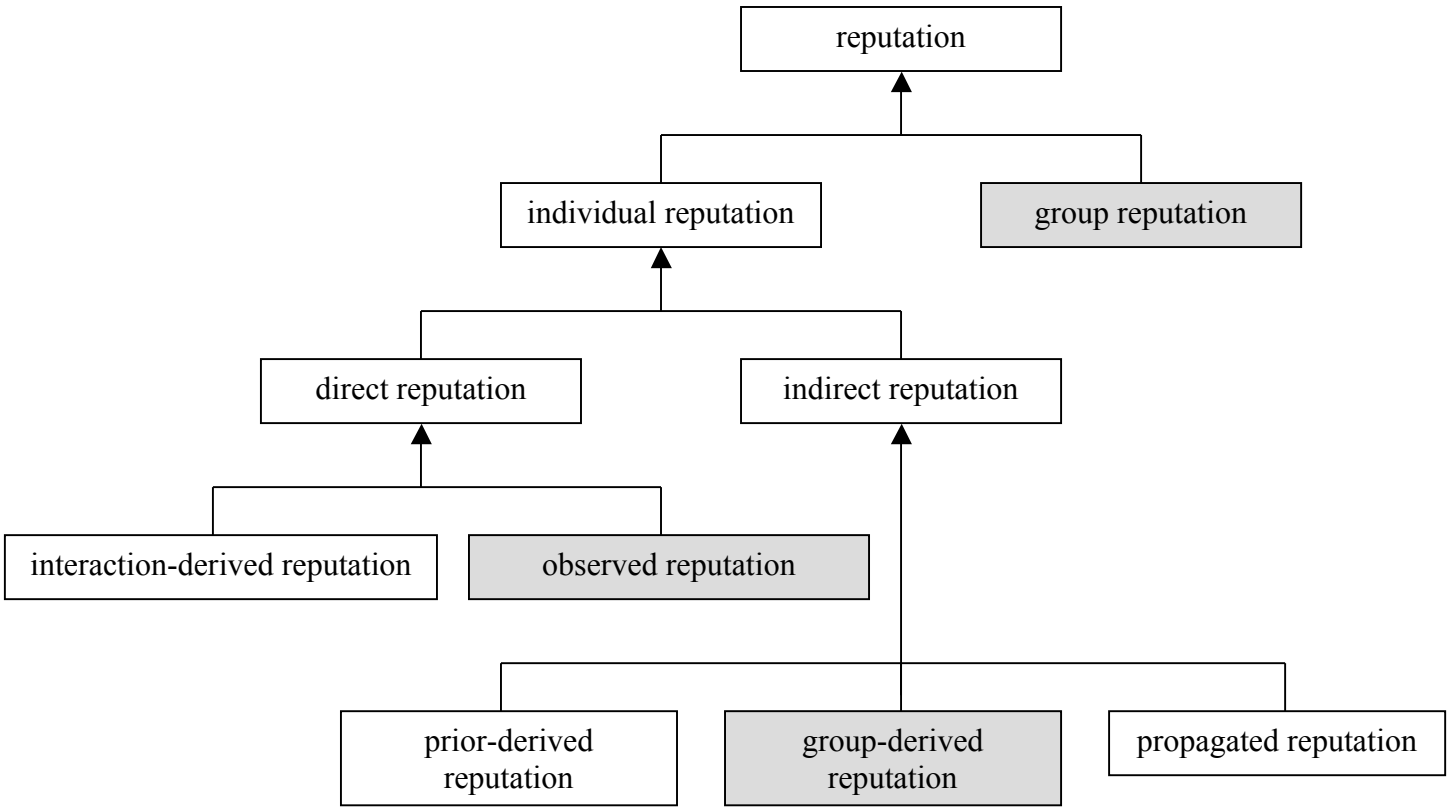

Abb. 4: Reputationsklassifikation. Die grau hinterlegten Boxen markieren Reputationsarten, welche geeignet sind durch globale Reputationswerte implementiert zu werden, bei den farblich nicht hinerlegten Boxen ist eine Implementierung durch personalisierte Reputationswerte eher geeignet. Quelle: [HaMM02]