

Ein Architektur-Modell für anonyme Autorisierungen und Überwachungsdaten *

Ulrich Flegel
FB4-LS6, Universität Dortmund, D-44221 Dortmund,
ulrich.flegel@udo.edu

Zusammenfassung: Eine digitale Welt benötigt Systeme, welche die Sicherheitsanforderungen von Dienstleistern und Nutzern gleichermaßen berücksichtigen. Dieser Beitrag betrachtet bei sicheren Autorisierungen die Anforderungen hinsichtlich Zurechenbarkeit und Anonymität mit Bezug auf eine Sicherheitsüberwachung bei der Dienstleistung. Hierfür wird ein Architektur-Modell für sichere anonyme Autorisierungen entwickelt, anhand dessen die Eigenschaften konkreter Anonymitäts-Technologien systematisch vergleichbar werden. Bekannte Ansätze für die Anonymisierung von Überwachungsdaten werden vorgestellt und verglichen.

1 Vom Realen des Digitalen: Ein Besuch im Zoo

Sicherheitsmaßnahmen in der digitalen Welt sind häufig bereits vorhandenen Sicherheitsmaßnahmen der realen Welt nachempfunden. Das mag daran liegen, daß Vertrauen letztlich stets in der realen Welt gegründet ist und Sicherheitsmaßnahmen gerade bei fehlendem Vertrauen der Akteure notwendig sind.

Wie wir in der realen Welt mit Vertrauen umgehen, läßt sich am Beispiel eines Studierenden zeigen, der den Zoo besuchen möchte. Der Zoo tritt hier als Dienstleister auf und bietet Studierenden kostenlosen Eintritt. Nicht-Studierende könnten versuchen, sich einen geldwerten Vorteil zu verschaffen, indem sie an der Zoo-Kasse lügen und sich in ihrer Eigenschaft als *Studierende* vorstellen. Der Besitz dieser Eigenschaft kann vom Kassenspersonal nicht vor Ort geprüft werden. Stattdessen wird verlangt, den Studierenden-Ausweis vorzuzeigen. Der Studierenden-Ausweis fungiert als beglaubigte Eigenschaftsaussage, indem er den Namen des Aussage-Subjekts der Eigenschaft *Studierender* zuordnet. Die Zoo-Kasse akzeptiert diese beglaubigte Eigenschaftsaussage, wenn gilt: Es wurde beschlossen, der vermerkten Universität als Agent für solche Beglaubigungen zu vertrauen, das Lichtbild "paßt" zur vorliegenden Person, der Studierenden-Ausweis ist noch nicht abgelaufen und sieht "echt" aus.

Wenn die Zoo-Kasse den Studierenden-Ausweis akzeptiert, autorisiert sie die vorliegende Person, den Zoo-Eingang zu passieren. Die Person erhält damit die dienstspezifische

*Die beschriebenen Arbeiten werden derzeit zum Teil von der Deutschen Forschungsgemeinschaft gefördert unter Bi 311/10-2.

Eigenschaft *Zoo-Eintritts-Berechtigter*. Die Zoo-Kasse stellt eine Autorisierung in Form eines Eintritts-Tickets aus. Am Zoo-Eingang wird das Eintritts-Ticket akzeptiert, wenn gilt: Der aufgedruckten Kasse wird vertraut, Tickets nur an Berechtigte auszustellen, die Ticket-Nummer “sieht plausibel aus”, das Ticket berechtigt zum Zoo-Eintritt, ist noch nicht abgelaufen und sieht “echt” aus.

Nach dem Zoo-Eingang springt dem Besucher ein Schild ins Auge, auf dem steht, welches Verhalten im Zoo untersagt ist. Vor allem soll man die Affen nicht ärgern, wohl weil die sich mit Bananenschalen-Geschossen rächen könnten. Der Zoo muß zunächst darauf vertrauen, daß die Zoo-Besucher sich an die Regeln halten. An kritischen Stellen (bei den Affen) kann der Zoo einen Wächter postieren, der Regel-Verstöße entdeckt und reagiert.

In diesem Beitrag wird das in [Fle03a] angedachte Architektur-Modell konkretisiert, anhand dessen die Eigenschaften konkreter Anonymitäts-Technologien erkennbar und verschiedene Architekturen im Hinblick auf anonyme Überwachungsdaten systematisch vergleichbar werden. Das Modell wird in drei Schritten entwickelt:

1) Ein PKI-basiertes Architektur-Modell für Autorisierungen [BK02] wird verallgemeinert, indem von der PKI-Technologie abstrahiert wird (Abschnitt 2). Dieses Modell berücksichtigt primär die Sicherheits-Interessen der Dienstleister.

2) Bestehende gesetzliche Verpflichtungen der Dienstanbieter zum Schutz der informationellen Selbstbestimmung der Dienstanutzer erschweren die überwachungsgestützte Absicherung von Diensten. Es wird ein Ansatz zum Interessenausgleich von Überwachung und Anonymität entwickelt, der auf Pseudonymen mit technischer Zweckbindung basiert (Abschnitt 3).

3) Durch die Kombination des Modells aus Abschnitt 2 mit Pseudonymen entsteht ein Architektur-Modell für anonyme Autorisierungen. Kriterien für den Vergleich von Architekturen für anonyme Autorisierung und Überwachung werden erarbeitet und im Modell angewandt (Abschnitt 4).

Mit dem Blick auf eine Sicherheitsüberwachung bei der Dienstleistung zeigt sich, daß ein Interessenausgleich insbesondere unter der hierfür spezifischen Anforderung der technischen Zweckbindung praktikabel nur durch die Pseudonymisierung bereits erhobener Überwachungsdaten machbar ist (Abschnitt 4). Bekannte Ansätze für die Pseudonymisierung von Überwachungsdaten werden vorgestellt und verglichen (Abschnitt 5).

2 Ein Architektur-Modell für Autorisierungen

Ausgehend von der Grundannahme, daß ein Dienst seinen Nutzern nicht hinsichtlich Aussagen über zugriffsrelevante Eigenschaften vertraut, arbeiten auch digitale Autorisierungs-Architekturen mit Eigenschaftsaussagen, die von vertrauenswürdigen Agenten verantwortlich beglaubigt werden. Im Modell werden Individuen, Rechner und andere Akteure eines verteilten IT-Systems als *Entitäten* bezeichnet. Ein *Prinzipal* ist ein Bit-String, der in seinem Anwendungsbereich eindeutig genau einer Entität als deren Surrogat zugeordnet ist. Eine Entität kann *Eigenschaften* haben, die in Sicherheitspolitiken als Entscheidungsbe-

dingungen formuliert sind. Der Begriff *Beglaubigung* bezeichnet im Modell den Vorgang und das Resultat, wenn ein verantwortlicher Agent als *Beglaubiger* eine Aussage über Eigenschaften beglaubigt, die entitätsbezogen und nicht dienstbezogen sind. Als Beispiel für die Beglaubigung über die Eigenschaft *Studierender* trat in Abschnitt 1 der Studierendenausweis auf. Der Begriff *Autorisierung* bezeichnet im Modell den Vorgang und das Resultat, wenn ein verantwortlicher Agent als *Autorisierer* eine Aussage über dienstspezifische Erlaubnisse beglaubigt. Als Beispiel für eine Autorisierung *Zoo-Eintritts-Berechtigter* trat in Abschnitt 1 das Eintritts-Ticket auf.

Eigenschaften werden einer *Subjekt-Entität* meist von einer anderen Entität, dem *verantwortlichen Agenten* zugeordnet (hier Universität oder Zoo-Kasse), indem der Agent eine Aussage über die Zuordnung eines Prinzipals des Subjekts zu Attributen, welche die Eigenschaften repräsentieren, unter einem seiner eigenen Prinzipale beglaubigt. Die Zuordnung des Subjekt-Prinzipals zur vorliegenden Entität wird mittels Authentisierungswerten verifizierbar gemacht. Die Eigenschaftsaussage enthält zusätzlich verifizierbare, unfälschbare Angaben zur Gültigkeit, die ausschließlich vom verantwortlichen Agenten aufgebracht werden können. Beglaubigte Eigenschaftsaussagen können in verschiedenen Formen auftreten, etwa als statisches Dokument (z.B. Zertifikate [BK02]) oder als interaktiver Protokollablauf. Die *Komponenten* einer Eigenschaftsaussage sind im einzelnen (s. Abb. 1): Ein Prinzipal des *verantwortlichen Agenten* für die Vertrauens-Evaluierung, *Validitätswerte* zur Verifikation der Gültigkeit, *Authentisierungswerte* zur Authentisierung der vorliegenden Entität, das als *Attribute* formulierte Eigenschaftsbündel der Subjekt-Entität für die Zugriffsentscheidungsfindung, sowie ein Prinzipal der *Subjekt-Entität* für die Verkettung von Eigenschaftsaussagen bei der Anfragebearbeitung.

Die Komponenten beglaubigter Eigenschaftsaussagen unterstützen im wesentlichen Sicherheitsziele im Sinne der Dienste. Dementsprechend stehen die in Abb. 2 hellgrau umrahmten Bereiche für die Durchsetzung der primär dienstbezogenen Sicherheitsziele und damit außerhalb der Kontrolle des Nutzers. Die Pfeile zeigen die Flußrichtung beglaubigter bzw. nachgewiesener Aussagen über Eigenschaften des Nutzers an¹. Die Pfeile werden im Text mittels ihrer Bezeichner referenziert (hier: A1 bis C2).

Die im Grundmodell² in Abb. 2 gezeigten Akteure sind die Verwaltung, ein Beglaubiger, ein Autorisierer und ein Dienst. Sie entsprechen z.B. bei *Kerberos* dem Client, dem *Authentication-Server*, dem *Ticket-Granting-Server* und dem Dienst-Server. Die Dienst-Nutzung verläuft in drei Phasen: 1) Der Nutzer läßt seine relevanten Eigenschaften beglaubigen (A1 bis A3 in Abb. 2). 2) Der Nutzer wird auf Vorlage der relevanten Beglaubigungen für die Dienst-Nutzung autorisiert (B1 bis B3 in Abb. 2). 3) Bei Vorlage dieser Autorisierungen kann der Nutzer den Dienst-Server in Anspruch nehmen (C1 und C2 in Abb. 2). Die *Verwaltung* wird vom Nutzer kontrolliert und wählt auf Grundlage der Nutzer-Politik und der Anforderungen des Agenten bzw. Dienstes (s. Politiken bei der Verifikation in Abb. 1) die für die jeweiligen Interaktionen zum Versand geeigneten Eigenschaftsaussagen aus.

¹Da die Antworten des Dienstes keine Aussagen über Eigenschaften des Nutzers enthalten, sind sie im Modell nicht zu sehen.

²Vom in Abb. 2 dargestellten Grundmodell lassen sich diverse praxisrelevante Varianten ableiten [Fle03b].

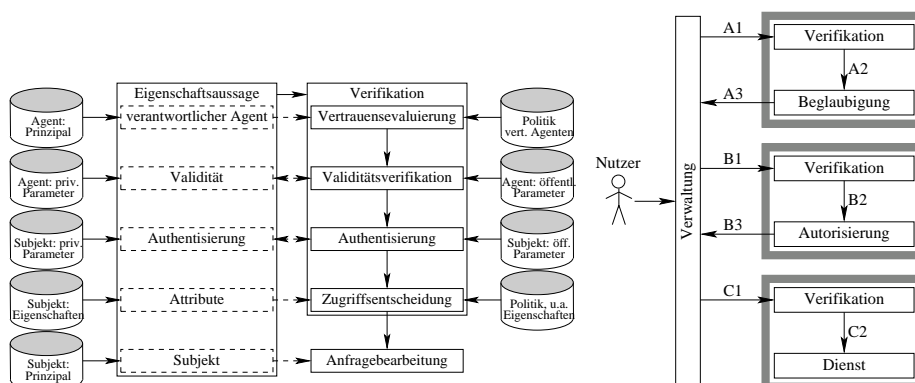


Abbildung 1: Eigenschaftsaussagen und deren Verifikation

Abbildung 2: Grundmodell

3 Pseudonyme mit zweckgebundener Aufdeckung

Audit-Daten werden auf Vorrat erhoben, gespeichert und analysiert mit dem Ziel, Mißbrauch zu entdecken und zwecks Rechtsverfolgung dem Urheber zuzurechnen (Wächter). Hier werden ausschließlich die vom Dienst erhobenen Audit-Daten betrachtet.

Bei der Verarbeitung von Audit-Daten kann der Zielkonflikt zwischen dem nutzerorientierten Interesse an Anonymität und dem dienstorientierten Interesse an Zurechenbarkeit durch die Dienstnutzung unter Pseudonymen im Sinne *mehrseitiger Sicherheit* fair gelöst werden, indem über die Kontrolle von Zusatzwissen zwischen Regelfall (keine Zurechenbarkeit) und Ausnahmefall (Zurechenbarkeit möglich) unterschieden wird. Die rechtliche Grundlage wird hier basierend auf [Jae00, RS00] vorausgesetzt und in [Fle03a, Fle03b] zusammengefaßt. Die verwendete Definition von *Pseudonymen* als Prinzipale, die per se ungeeignet sind, die jeweils zugeordnete Entität zu identifizieren, greift auf die in [PK00] vorgeschlagenen Definitionen für *Unverkettbarkeit* und *Anonymität* zurück. Die darauf aufbauenden Begriffe der *Pseudonymisierung* mit Hilfe einer *Zuordnungsregel* und die spätere *Aufdeckung* bzw. *Reidentifizierung* werden hier intuitiv verwendet und in [Fle03b] präzisiert.

Die *kontrollierte Aufdeckbarkeit* von Pseudonymen stellt eine kontrollierte Möglichkeit dar, pseudonymisierte Objekte von ihrem anonymen Zustand in einen zurechenbaren Zustand zu überführen. Diese Möglichkeit wird über die Kenntnis der Zuordnungsregel kontrolliert. Wenn die Verantwortung über den Umgang mit der Zuordnungsregel einer Person übertragen wird, findet bei der Reidentifizierung eine *organisatorische Zweckbindung* statt. Da diese Person vor der Aufdeckung idR. eine manuelle Zweckprüfung durchführen muß, kann sich die Pseudonym-Aufdeckung bei organisatorischer Zweckbindung stark verzögern. Der Zweck der Aufdeckbarkeit kann auch bereits in die Erzeugung der Pseudonyme eingehen, indem man die Zuordnungsregel in geschützter Form den pseudonymisierten Daten beifügt. Der Zweck bestimmt, unter welchen Bedingungen dieser Schutz

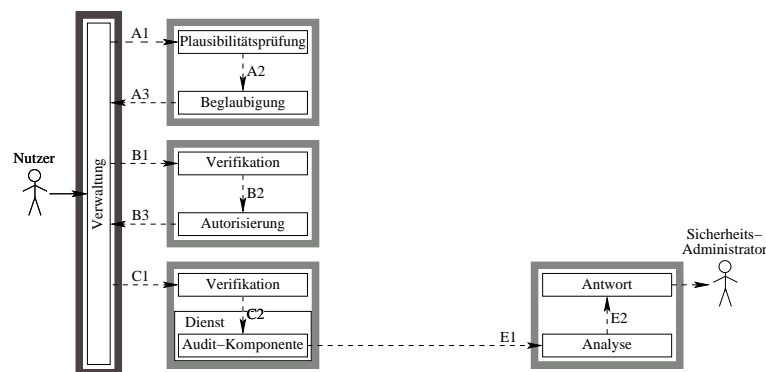


Abbildung 3: Einseitig sicher: Anonymität durch die Verwaltung

unwirksam ist und die Zuordnungsregel zur Reidentifizierung genutzt werden kann. Paßt man die Zuordnungsregel bei der Pseudonym-Erzeugung kryptographisch diesen Bedingungen an, erhält man Pseudonyme mit unumgehbarer, *technisch zweckgebundener* Aufdeckbarkeit.

4 Ein Architektur-Modell für anonyme Autorisierungen

Die Verifikation beglaubigter Eigenschaftsaussagen bedarf in vielen Fällen keiner identifizierenden Prinzipale. So können Eigenschaftsaussagen anonymisiert werden, indem der Subjekt-Prinzipal durch ein Pseudonym mit geeigneten Eigenschaften ersetzt wird (s. Abschnitt 3). Das deutsche Signaturgesetz sieht bereits entsprechende Beglaubigungen vor (§7 Abs. 1-3 SigG) [RS00]. Entsprechend ist es etwa an der Zoo-Kasse nicht notwendig, den Namen des Studierenden zu erfahren. Wichtig ist nur, daß die Eigenschaft *Studierender* an die Person gebunden ist, die einen gültigen Studierenden-Ausweis vorlegt, und daß dieser von einem vertrauenswürdigen Agenten ausgestellt wurde. Also könnte der Studierenden-Ausweis anonym ausgelegt werden, indem in die Subjekt-Komponente statt des Namens die Matrikel-Nummer des Studierenden eingetragen würde.

Der Agent ist nun einerseits im Interesse der Zurechenbarkeit den Verwendern der Eigenschaftsaussage gegenüber zusätzlich dafür verantwortlich, daß er entsprechend seiner im voraus festgelegten Politik zu spezifischen Zwecken gegenüber spezifischen Entitäten mittels der Zuordnungsregel Pseudonyme aufdeckt. Andererseits ist der Agent im Interesse der Anonymität den Subjekt-Entitäten gegenüber dafür verantwortlich, die Zuordnungsregel zu schützen und hinsichtlich der Aufdeckbarkeit und Verkettbarkeit der Pseudonyme seine dem Subjekt bekannte Politik einzuhalten.

Folgend werden auf Abschnitt 2 basierend Architekturen vorgestellt, die Nutzer-Anonymität gegenüber den *Sicherheits-Administratoren* eines Dienstes herstellen, welche Beobachtungen ausschließlich auf der Basis der vom Dienst gelieferten Audit-Daten machen können (s. Abb. 3 bis Abb. 6). Die Audit-Daten werden von der *Audit-Komponente* des Dienstes erhoben und der *Audit-Analyse* der Sicherheits-Administratoren des Dienstes

verfügbar gemacht (E1 in Abb. 3). Diese erzeugt entsprechend des *Analyse-Zwecks Einzelberichte* und sendet sie an die *Antwort-Einheit* (E2 in Abb. 3), welche wiederum geeignet auf die Einzelberichte reagiert. Eine konkrete Instanz dieses Szenarios wäre ein Intrusion-Detection-System, dessen Analyse-Zweck das Entdecken bekannter und durch die Dienstnutzer verursachter Anfangsverdachte für *Schutzzielverletzungen* bzw. Mißbräuche ist.

Die Abb. 3 bis Abb. 6 zeigen die dem Modell aus Abb. 2 entsprechenden anonymen Versionen, bei denen eine Entität Anonymität der Dienst-Nutzer gegenüber den Sicherheits-Administratoren herstellt, indem sie ein Nutzer-Pseudonym erstmalig einführt, bevor die Audit-Daten die Audit-Analyse erreichen.

In den Abbildungen zeigen die *durchgezogenen Pfeile* die Flußrichtung zurechenbarer und beglaubigter bzw. nachgewiesener Aussagen über Eigenschaften an. Die *gestrichelten Pfeile* zeigen die Flußrichtung der anonymen und ggf. beglaubigten Aussagen über Eigenschaften an. Schließlich zeigen die *gepunkteten Pfeile* die Flußrichtung der Zuordnungsregel an. Jede fette graue Umrahmung schließt einen Bereich ein, in dem die Interessen einer Entität durchgesetzt werden. In diesem Bereich dürfen jene Entitäten keine Kontrolle ausüben, deren Interessen mit den im Bereich durchgesetzten Interessen im Konflikt stehen. Dabei stehen die dunkelgrauen Umrahmungen für das Nutzerinteresse Anonymität und die hellgrauen Umrahmungen für das Interesse der Sicherheits-Administratoren an Zurechenbarkeit. Dunkel ausgefüllte Kästen realisieren gemeinsam mehrseitige Sicherheit. Sie befinden sich gerade in den doppelt umrahmten Bereichen, also dort, wo konfligierende Interessen durchgesetzt werden.

Einseitige Sicherheit kann zugunsten der Anonymität entstehen, wenn der Beglaubiger die von der Verwaltung des Nutzers ausgewählten Subjekt-Prinzipale nicht daraufhin prüft, daß sie tatsächlich identifizierende Prinzipale des Nutzers sind. Wenn er solche Eigenschaftsaussagen akzeptiert, ließen diese sich nicht verlässlich aufdecken, weil die zugehörige Zuordnungsregel unter der Kontrolle der Verwaltung des Nutzers steht, dem die Sicherheits-Administratoren nicht hinsichtlich Zurechenbarkeit vertrauen (s. Abb. 3).

Da in mehrseitig sicheren Versionen gegenläufige Interessen mehrerer Entitäten berücksichtigt werden sollen, führt dies zum Ausschluß der Kontrolle eben dieser Entitäten über die Interessenobjekte, also die Pseudonyme in den Eigenschaftsaussagen. Entsprechend ist für mehrseitige Sicherheit die Zuordnungsregel von Agenten zu kontrollieren, denen die Interessenträger vertrauen müssen. Diese Situation ist in Abb. 4 bis Abb. 6 dargestellt.

In Abb. 4 bis Abb. 6 sind nur Architekturen für Pseudonyme mit organisatorischer Zweckbindung und die dafür notwendigen Kontrollverhältnisse dargestellt. Abb. 7b zeigt am Beispiel eines Dienstes mit einem Pseudonymisierer, wie der Einsatz der technischen Zweckbindung für die kontrollierte Aufdeckbarkeit die notwendigen Kontrollverhältnisse vereinfacht³. Bei der technischen Zweckbindung der Aufdeckbarkeit wird den Pseudonymen die zweckgebunden geschützte Zuordnungsregel beigelegt (E2 in Abb. 7b), so daß diese nicht mehr direkt dem Reidentifizierer übermittelt werden muß (vgl. R1 in Abb. 7a). Die Reidentifizierung ist so unumgebar nur noch entsprechend dem Zweck der kontrollierten Aufdeckung möglich. Demgemäß muß der Nutzer derjenigen Entität, welche die Reidenti-

³Im Modell ist eine technische Zweckbindung analog für Beglaubiger und Autorisierer möglich (s. Abb. 4 und Abb. 5), aber unterschiedlich sinnvoll.

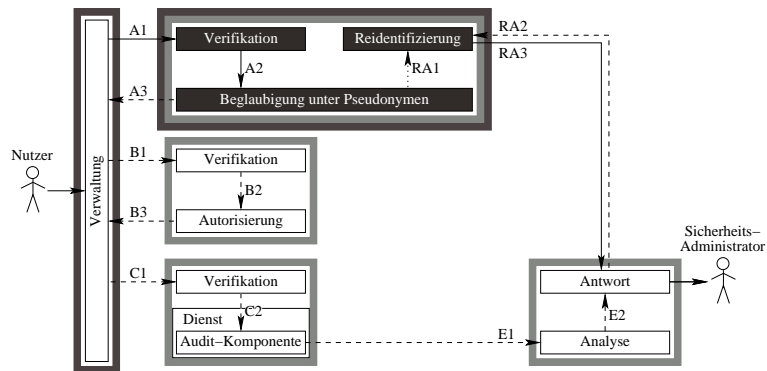


Abbildung 4: Mehrseitig sicher: Anonymität und Zurechenbarkeit durch den Beglaubiger

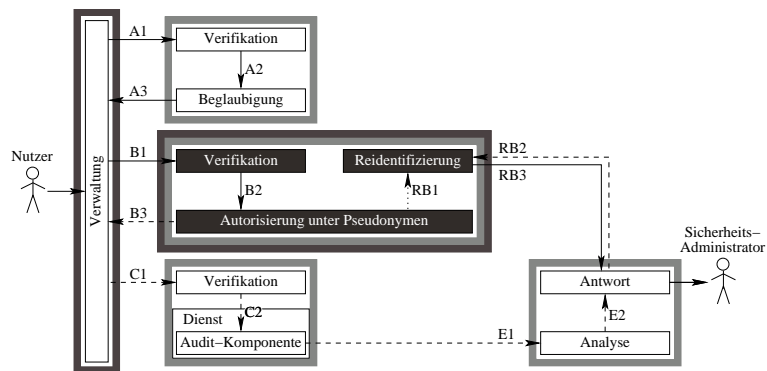


Abbildung 5: Mehrseitig sicher: Anonymität und Zurechenbarkeit durch den Autorisierer

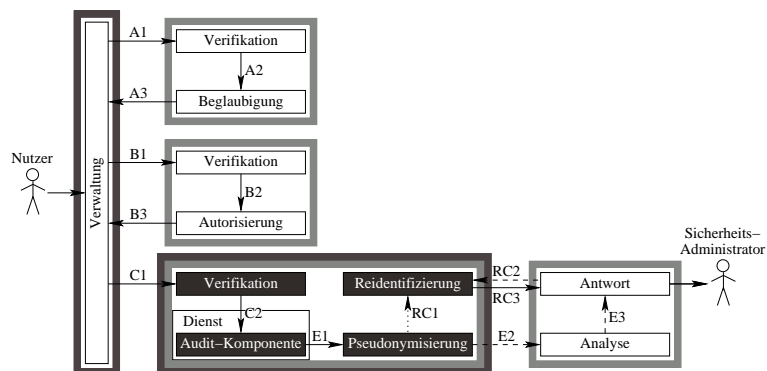


Abbildung 6: Mehrseitig sicher: Anonymität und Zurechenbarkeit durch den Dienst

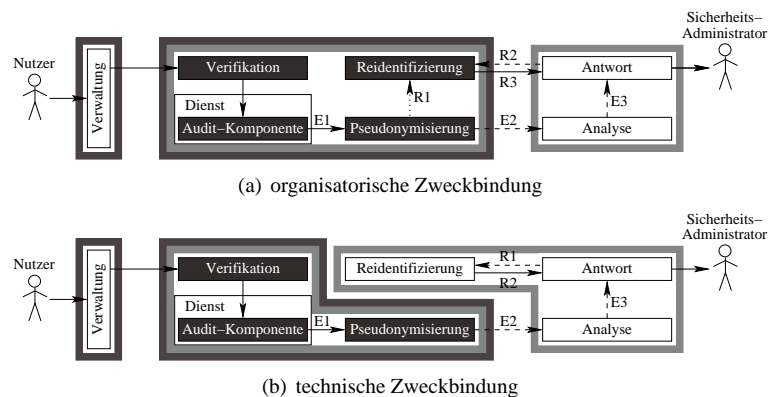


Abbildung 7: Zweckbindung der kontrollierten Aufdeckbarkeit

fizierung kontrolliert, nicht mehr vertrauen. Da also die Sicherheits-Administratoren nicht mehr von der Kontrolle des Reidentifizierers ausgeschlossen sind, können sie die Reidentifizierung selbst kontrollieren und unverzüglich durchführen, sobald der entsprechende Zweck vorliegt.

Architekturen für anonyme Autorisierungen im Vergleich:

Die Abb. 3 bis Abb. 6 zeigen die verschiedenen Entitäten, die Pseudonyme einführen können, so daß die Audit-Analyse nur anonyme Audit-Daten erhält. Dabei hat das Einführen der Pseudonyme bei jeder Entität spezifische Vor- und Nachteile, welche im Folgenden diskutiert und in Tabelle 1 zusammengefaßt werden.

Mehrseitige Sicherheit kann mit Hilfe jener Entitäten erreicht werden, die nicht selbst Träger der konfligierenden Interessen sind. Auch wenn die Entität kein Interessenträger ist könnte sie sich parteiisch verhalten, wenn die Organisation, der sie abhängig angehört, Träger eines Interesses ist. Deswegen ist *Dienst-Unabhängigkeit* der Entität im Interesse der Anonymität vorzuziehen. Man versucht in der realen Welt durch organisatorische Maßnahmen parteiisches Verhalten zu vermeiden, indem es eine Person in der Organisation gibt, welche das Nutzerinteresse vertritt, etwa der Datenschutz-Beauftragte. Eine *vertrauenswürdige Attributzuordnung*, also ob die hinter einer pseudonymen Eigenschaftsaussage verborgene Person tatsächlich die angegebenen Eigenschaften besitzt, ist eher zu erwarten, wenn ein Agent, der auch die Interessen des Dienstes wahrt, für die Eigenschaftsaussage verantwortlich ist. Wie bei Diensten ist eine *technische Zweckbindung* analog für Autorisierer möglich. Da jedoch Beglaubigungen zur Erlangung von Autorisierungen für viele verschiedene Dienste geeignet sind, müßten entsprechend viele Verarbeitungs-Zwecke antizipiert und berücksichtigt werden. Aufgrund dieser Erosion der Anonymität der Beglaubigungen erscheint eine technische Zweckbindung durch Beglaubiger nicht sinnvoll. Werden Pseudonyme im Modell noch vor dem Dienst-Zugriff eingeführt, kann die *Pseudonymverifikation vor dem Zugriff* stattfinden. Anfragen mit ungültigen Eigenschaftsaussagen können zur Schadensvermeidung abgewiesen werden. Wenn die Entität, welche die Pseudonyme einführt, auf ein entsprechendes Software-Gegenstück beim Nutzer oder auf die

Tabelle 1: Übersicht über die Eigenschafts-Kriterien, gruppiert nach inhaltlichem Bezug zu Vertrauen, operationaler Sicherheit und Praktikabilität. Kriterium ist: ‘√’=erfüllt, ‘-’=nicht erfüllt, ‘%’=gegenstandslos

Eigenschafts-Kriterien	Pseudonym-ausgebende Entität			
	Verwaltung	Beglaubiger	Autorisierer	Dienst
Mehrseitige Sicherheit	-	√	√	√
Dienst-Unabhängigkeit	√	√	-	-
Vertrauenswürdige Attributzuordnung	-	√	√	%
Technische Zweckbindung	-	-	√	√
Pseudonymverifikation vor Zugriff	√	√	√	-
Nutzer-Unabhängigkeit	-	-	-	√
Infrastruktur-Unabhängigkeit	√	-	-	√

korrekte Bedienung durch den Nutzer angewiesen ist, eröffnet dies einerseits durch Fehlbedienung Risiken für die Anonymität. Andererseits hat der Dienst ein Interesse daran, daß die Audit-Daten anonym vorliegen, um nicht die gesetzlichen Datenschutz-Anforderungen erfüllen zu müssen. *Nutzer-Unabhängigkeit* ist daher beidseitig von Vorteil. Kommen beglaubigte Eigenschaftsaussagen zum Einsatz, erfordert dies eine Infrastruktur zur Nutzerregistrierung. Der erforderliche Etablierungsaufwand kann in der Praxis ein beträchtliches Hindernis darstellen. Deshalb dient *Infrastruktur-Unabhängigkeit* einer raschen Umsetzung.

Beispiele:

Eine Anforderung bei der Analyse von Audit-Daten hinsichtlich Anhaltspunkten für Mißbrauch ist die zeitnahe Pseudonym-Aufdeckbarkeit zwecks Zurechenbarkeit. Unter dem Gesichtspunkt der Praktikabilität sind die Unabhängigkeit der Lösung vom Nutzer und die Unabhängigkeit von aufwendigen Infrastrukturen entscheidend. Tabelle 1 zeigt, daß diese Anforderungen gemeinsam nur auf Dienstebene erfüllbar sind. Die hierfür bekannten Ansätze werden im Folgenden vorgestellt und in Abschnitt 5 miteinander verglichen. Beispiele für datenschutzfördernde Technologien, die Anonymität in der Rolle der anderen Entitäten implementieren, sind in der Langfassung dieses Beitrags zu finden [Fle03b].

Mit dem teilimplementierten Forschungs-System *Intrusion Detection and Avoidance (IDA)* wurde das Konzept der Intrusion-Detection-Analyse auf anonymen Audit-Daten eingeführt [FH93]. Das Forschungs-System *Adaptive Intrusion Detection (AID)* greift das mit IDA eingeführte Konzept bei jedoch stark verschiedener Architektur auf [MH00]. *Lundins Firewall Audit Anonymisierer* ist ein Forschungs-System für die Anonymisierung der Audit-Daten einer spezifischen Proxy-Firewall. Auf den anonymisierten Daten wurden Intrusion-Detection-Experimente durchgeführt [LJ00]. *Jaegers Anonymisierungs-Konzept* bietet verkettbare Pseudonyme, die nicht kontrolliert aufgedeckt werden können. Sie können aber zur Bestätigung eines konkreten Verdachts hinsichtlich eines identifizierenden Prinzipals dienen [Jae00]. Das kommerzielle Content-Filter-System *WebWasher* kann seine Audit-Daten bzw. Berichte anonymisieren und unterstützt eine organisatorische Zweckbindung bei der kontrollierten Aufdeckung [wA03]. Das frei verfügbare Forschungs-System *BSMpseu* anonymisiert Solaris-BSM-Audit-Daten mittels verkettbarer Pseudonyme ohne eine Möglichkeit zur kontrollierten Aufdeckung. Auf den anonymisierten Daten

Tabelle 2: Übersicht über die Eigenschaften der Ansätze für anonyme Audit-Daten.
 ‘√’=Kriterium erfüllt, ‘-’=Kriterium nicht erfüllt, ‘%’=fehlende Information zum Ansatz,
 ‘(?...?)’=Vermutung.

Ansatz (Verfügbarkeit)	Aufdeckung möglich	Verkettung möglich · Pseudonym-Sorte
	Art der Zuordnungsregel	zusätzliche Pseudonym-Wechsel
	Art der Zweckbindung · Schutz	technische Zweckbindung
	Kontrolle der Zweckbindung	Kontrollierende Entität
	Architektureigenschaften: Ursache	
Anonyme Log File Anonymizer (Forschung)	-	-
	Vergrößerung	-
	-	-
	-	Datenschützer
	einseitig, Anonymität: keine Aufdeckbarkeit	
BSMpseu (Forschung, frei)	-	√ · Subjekt-Pseudonyme
	Zufall	-
	-	-
	-	Datenschützer
	einseitig, Anonymität: keine Aufdeckbarkeit	
Jaeger- Anonymisierung (Konzept)	-	√ · Subjekt-Pseudonyme
	Einwegfunktion (Hash)	-
	-	-
	-	Datenschützer
	einseitig, Anonymität: keine Aufdeckbarkeit	
Lundin Firewall Audit Anonymizer (Forschung)	√	√ · Subjekt-Pseudonyme
	Zähler / Vergrößerung	Zuordnung vergessen
	-	-
	Sicherheits-Admin	Datenschützer
	einseitig, Zurechenbarkeit: Angreifer kennt die Zuordnungsregel	
WebWasher (kommerziell)	√	% (?√ · Subjekt-Pseudonyme?)
	% (?Chiffrieren?)	%
	organisatorisch (?nur einmal?)	% (?-?)
	% (?Datenschützer?)	% (?Datenschützer?)
	% (?ggf. einseitig, Zurechenbarkeit: 4-Augen-Prinzip umgehbar?)	
IDA – Intrusion Detection and Avoidance (Konzept)	√	√ · Subjekt-Pseudonyme
	symmetrisches Chiffrieren	Schlüssel-Wechsel
	organisatorisch (nur einmal)	-
	Datenschützer	Datenschützer
	ggf. einseitig, Zurechenbarkeit: 4-Augen-Prinzip umgehbar	
AID – Adaptive Intrusion Detection (Forschung)	√	√ · Subjekt-Pseudonyme
	symmetrisches Chiffrieren	Schlüssel-Wechsel
	- / organisatorisch	-
	- / Datenschützer	Datenschützer
	einseitig, Zurechenbarkeit: Angreifer kennt die Zuordnungsregel	
Pseudo/CoRe – Pseudonymization with Conditional Reidentification (Forschung, frei)	√	√ · Rollen-Pseudonyme
	symmetrisches Chiffrieren	Timeout oder Verdachtsabbruch
	techn. + org. · Geheimnisteilung	-
	Datenschützer	Datenschützer
	mehrseitig, Anonymität und Zurechenbarkeit	

wurden Intrusion-Detection-Experimente durchgeführt [Rie03]. Der *Anonimouse Log File Anonymizer* anonymisiert Web-Server-Audit-Daten unter Beibehaltung der Top-Level-Domains von Nutzer-Adressen. Eine kontrollierte Aufdeckung ist nicht möglich [EP01]. Das frei verfügbare Forschungs-System *Pseudonymization with Conditional Reidentification (Pseudo/CoRe)* anonymisiert Audit-Daten im Sinne mehrseitiger Sicherheit. Dabei unterliegen die Pseudonym-Nutzungskontexte, der Pseudonym-Wechsel und die kontrollierte Pseudonym-Aufdeckung der technischen Zweckbindung [Fle03c, Fle02].

5 Anonyme Audit-Daten

Das nachträgliche Pseudonymisieren von Audit-Daten erzielt eine vergleichbare Wirkung wie die Dienstnutzung mittels pseudonymer Autorisierungen [RS00]. Allerdings stellt die spezifische Anwendungssituation andere Anforderungen an die Pseudonym-Erzeugung. *Performanz:* Je nach Sorte des Dienstes kann ein extrem hohes Audit-Daten-Aufkommen zu bewältigen sein. Die Pseudonym-Erzeugung findet idealerweise on-the-fly statt und sollte daher einen dem Datenaufkommen angemessenen Durchsatz erreichen. Im Idealfall findet die Anonymisierung auf dem Gerät statt, das die Nutzeranfragen zur Diensterbringung verarbeitet. Die Pseudonym-Erzeugung sollte daher nicht den überwiegenden Teil der Prozessor-Ressourcen binden. Aufwendige kryptographische Verfahren für die Pseudonym-Erzeugung scheiden daher für einen dienst-lokalen on-the-fly-Einsatz aus. *Verwendungszweck:* Erfordert der Zweck eine rasche kontrollierte Aufdeckbarkeit, läßt sich dies verläßlich nur mittels technischer Zweckbindung erreichen.

Audit-Daten-Anonymisierer im Vergleich:

Die in Abschnitt 4 vorgestellten Ansätze für anonyme Audit-Daten werden im Folgenden anhand der Eigenschaften ihrer Pseudonyme (s. Abschnitt 3, [PK00]) und den notwendigen Kontrollverhältnissen (s. Abschnitt 4) in Tabelle 2 verglichen. Alle betrachteten Ansätze berücksichtigen die oben formulierte Performanz-Anforderung. Im Bereich der Architektureigenschaften liegen die größten Probleme der ursprünglich für mehrseitige Sicherheit ausgelegten Ansätze. Entweder wurden die Vertrauensbeziehungen und Kontrollverhältnisse beim Entwurf nicht vollständig berücksichtigt, so daß der Sicherheits-Administrator unter Umgehung der Zweckbindung direkten Zugriff auf die Zuordnungsregel erlangen kann. Oder es wurde ein ungeeignetes Verfahren zur Implementierung des 4-Augen-Prinzips gewählt, so daß der aufgeteilte Dechiffrier-Schlüssel nach der ersten Aufdeckung zumindest einer der beiden Entitäten bekannt ist.

Fazit

Anhand der vorgestellten Modelle lassen sich die Eigenschaften existierender Architekturen für anonyme Autorisierungen bestimmen und vergleichen. Auf Ebene des Dienstes läßt sich dies praktikabel durch Audit-Daten-Anonymisierer erreichen. Beim Entwurf bzw. bei der Auswahl von Audit-Daten-Anonymisierern ist besonderes auf die notwendigen Kontrollverhältnisse und die Mechanismen für die Durchsetzung der Zweckbindung bei der Pseudonym-Aufdeckung zu achten.

Literaturverzeichnis

- [BK02] Joachim Biskup and Yücel Karabulut. A Hybrid PKI Model with an Application for Secure Meditation. In *Proceedings of the Annual IFIP WG 11.3 Working Conference on Data and Application Security*, Cambridge, England, July 2002.
- [EP01] Claudia Eckert and Alexander Pircher. Internet Anonymity: Problems and Solutions. In Michel Dupuy and Pierre Paradinas, editors, *Proceedings of the IFIP TC11 16th International Conference on Information Security (IFIP/Sec'01)*, pages 35–50, Paris, France, June 2001. IFIP, Kluwer Academic Publishers.
- [FH93] Simone Fischer-Hübner. *IDA (Intrusion Detection and Avoidance System): Ein einbruch-sentdeckendes und einbruchsvermeidendes System (in German)*. Shaker, 1993.
- [Fle02] Ulrich Flegel. Pseudonymizing Unix Log Files. In George Davida, Yair Frankel, and Owen Rees, editors, *Proceedings of the Infrastructure Security Conference (InfraSec2002)*, number 2437 in LNCS, pages 162–179, Bristol, United Kingdom, October 2002. Springer.
- [Fle03a] Ulrich Flegel. Anonyme Audit-Daten im Überblick (in German). *Datenschutz und Datensicherheit*, 27(5):278–281, May 2003.
- [Fle03b] Ulrich Flegel. Ein Architektur-Modell für anonyme Autorisierungen und Überwachungsdaten (in German). Technical report, Dept. of Computer Science, Chair VI Information Systems and Security, June 2003. Extended version of this paper. <http://ls6-www.cs.uni-dortmund.de/issi/archive/literature/2003/Flegel:2003d.pdf>.
- [Fle03c] Ulrich Flegel. Praktikabler Datenschutz für Log-Daten (in German). In Rolf Schaumburg and Marco Thorbrügge, editors, *Proceedings of the 10th DFN-CERT Workshop on Sicherheit in vernetzten Systemen*, DFN-CERT publications, pages F1–F20, Hamburg, Germany, February 2003. DFN-CERT, Books on Demand.
- [Jae00] Stefan Jaeger. Verbotene Protokolle (in German). *Zeitschrift für Kommunikations- und EDV-Sicherheit (KES)*, 2000(5):6–12, 2000.
- [LJ00] Emilie Lundin and Erland Jonsson. Anomaly-based intrusion detection: privacy concerns and other problems. *Computer Networks*, 34(4):623–640, October 2000.
- [MH00] Michael Meier and Thomas Holz. Sicheres Schlüsselmanagement für verteilte Intrusion-Detection-Systeme (in German). In Patrick Horster, editor, *Systemsicherheit*, DuD-Fachbeiträge, pages 275–286, Bremen, Germany, March 2000. GI-2.5.3, ITG-6.2, ÖCG/ACS, TeleTrusT, Vieweg.
- [PK00] Andreas Pfitzmann and Marit Köhntopp. Anonymity, Unobservability, and Pseudonymity – A Proposal for Terminology. In Hannes Federrath, editor, *Proceedings of the international Workshop on Design Issues in Anonymity and Unobservability*, number 2009 in LNCS, pages 1–9, Berkeley, California, July 2000. ICSI, Springer.
- [Rie03] Konrad Rieck. *Konzept zur datenschutzorientierten Verarbeitung von Solaris-BSM-Audit-Daten (in German)*. Fachbereich Mathematik und Informatik, Institut für Informatik, Freie Universität Berlin, January 2003. <http://www.roqe.org/bsmpseu>.
- [RS00] Alexander Roßnagel and Philip Scholz. Datenschutz durch Anonymität und Pseudonymität (in German). *Zeitschrift für Informations-, Telekommunikations- und Medienrecht (MMR)*, 2000(12):721–732, 2000.
- [wA03] webwasher.com AG. Den Überblick behalten, Reporting mit WebWasherEE (in German). http://www.webwasher.com/product_pdf/deutsch/Produktblatt_Reporting.pdf, January 2003.