

Verteiltes Filtern mit Contags und Sicherheits-Labeln

Matthias Kabatnik¹, Reiner Sailer²

¹ Institut für Nachrichtenvermittlung und Datenverarbeitung, Universität Stuttgart

² IBM Research, T. J. Watson Research Center, Yorktown Heights, NY, USA

kabatnik@ind.uni-stuttgart.de, sailer@watson.ibm.com

Abstract

Im Zuge der Globalisierung von Netzdiensten haben sich sehr heterogene Netzstrukturen entwickelt. Teilnetze unterschiedlicher Technologien und unterschiedlicher Verantwortlichkeiten werden zusammengeschaltet. Dabei sind ernstzunehmende Sicherheitsprobleme entstanden, deren Lösung bis heute zu erheblichen Einschränkungen des über Netzgrenzen gelenkten Verkehrs führt.

Dieser Beitrag stellt ein neues Zugriffskontroll-Verfahren vor, das die Übergänge zwischen Teilnetzen mit feinerer Granularität absichert. Unser Verfahren arbeitet auf Netzebene und erweitert das bislang verwendete Filtern sowohl um Filterkriterien, z.B. basierend auf Integritäts- und Vertraulichkeitsklassen, als auch um Kontextinformation. Sicherheits-Label speichern Sicherheitsklassen für Daten im Datenpaket selbst. Sie bilden die Grundlage für ein Zugriffskontrollverfahren, das unabhängig von Benutzern und Rechnerknoten arbeitet. Context-Tags (Contags) speichern Kontext-Informationen (Meta-Information) direkt im Datenpaket, z.B. ob das Datenpaket geschützt empfangen wurde (z.B. durch IPSec/IKE) oder über welchen Link Daten empfangen wurden (z.B. Incoming Linkset). Contags ermöglichen verteiltes Filtern, da sie die für das Filtern relevanten Meta-Informationen erhalten (Historie). Das hier vorgestellte Zugriffskontroll-Verfahren implementiert eine verteilte und zustandslose Filterung. Wir wenden es auf IP-basierte Netze und auf Signalisierernetze an.

1 Einführung

Die Vernetzung von Computersystemen und der Einsatz verteilter Anwendungen ermöglichen eine Vielzahl neuer, flexibler Dienste. Gleichzeitig entstehen jedoch neue Herausforderungen bezüglich der Sicherheit der Information, die zwischen verteilten Anwendungen über Netze ausgetauscht wird. Insbesondere wenn die Vernetzung in großem, nicht mehr unmittelbar überschaubarem Maßstab erfolgt, müssen zusätzliche Schutzmaßnahmen getroffen werden.

Ein aktuelles Beispiel ist die Kopplung (Interconnection) verschiedener TCP/IP-Teilnetze einer Firma über den öffentlichen Bereich des Internets. Dort sind Schutzmaßnahmen notwendig, da sonst vertrauliche Daten ausgespäht oder manipuliert werden könnten oder Systeme durch unautorisiertes Einspielen von Daten in ihrer Integrität bedroht würden. Ein weiteres aktuelles Beispiel ist die Kopplung von SS7¹-Signalisierernetzen eines Betreibers bei gleichzeitiger Anbindung von Fremdnetzen.

1. SS7: Das Signalisiersystem Nr. 7 wird zum Austausch von Steuer- und Management-Daten in öffentlichen Fernsprechnetzen angewendet, z.B. im ISDN und im GSM.

Wir stellen in diesem Beitrag ein Verfahren vor, das zum Schutz heterogener Netzstrukturen auf Netzebene eingesetzt werden kann. Das Verfahren basiert darauf, größere heterogene Netze in kleinere – aus Sicherheitssicht homogene – Teilnetze zu zerlegen. Diese Teilnetze werden intern unabhängig geschützt. Die Übergänge zwischen Teilnetzen werden durch zusätzliche Zugriffskontroll-Mechanismen überwacht. Zur Strukturierung von heterogenen Netzen wird das *Domänen-Konzept* herangezogen [10]. Dieses Konzept unterscheidet Domänen hinsichtlich sicherheitsrelevanter Eigenschaften, z.B. Verantwortlichkeiten, physikalischer Schutz, Steuerungs-Software, Zugangspunkte. Nachfolgend wird unter einer Domäne ein Bereich verstanden, der durch Einsatz von Sicherheitsmaßnahmen an den Bereichsgrenzen von seinen umgebenden Bereichen sicherheitstechnisch unabhängig ist (autonom). Beispiele autonomer Bereiche stellen durch Firewalls geschützte LAN-Segmente oder durch physikalische Separation und Nachrichtenfilter geschützte öffentliche Netze (z.B. SS7-Signalisiernetze des ISDN) dar.

Innerhalb einer Domäne lassen sich Schutzziele festlegen (Sicherheitsanforderungen bezogen auf Objekte), die durch innerhalb der Domäne implementierte Schutzvorkehrungen garantiert werden. Ein ISDN-Netzbetreiber kann beispielsweise Schutzziele innerhalb seines Netzes durch entsprechende Zugangskontrollen und Sicherheitsfunktionen autonom durchsetzen. An den Übergangspunkten zu *angrenzenden Domänen* muß sichergestellt werden, daß Informationsströme zwischen den Domänen keine Schutzziele des Ursprungs- oder Ziel-Bereiches verletzen. Z. B. sollen Management- oder Tarifierungsinformationen aus fremden Netzen nicht verarbeitet werden, falls sie ungeschützt über unsichere Bereiche übertragen wurden oder in nicht vertrauenswürdigen Bereichen entstanden sind.

Die Zusammenschaltung von unabhängig gesicherten Teilbereichen und der Schutz bereichsübergreifender Informationsströme und Ressourcen stellen die zentralen Punkte dieses Beitrags dar. Bild 1 veranschaulicht das Prinzip der Zusammenschaltung: Wird ein Datum von einem Netzbereich A in einen Netzbereich B übertragen und werden an dieses Datum bestimmte Anforderungen wie Vertraulichkeit oder Integrität gestellt, so muß der Übergangspunkt zwischen den Teilbereichen A und B sicherstellen, daß die Anforderungen trotz bereichsübergreifender Kommunikation eingehalten werden. Dies erfolgt entweder durch ein a-priori Wissen des Prüfpunktes (Policy-Information) oder durch entsprechenden vorsorglichen Schutz der Daten durch Verschlüsselung oder Signierung zur Überbrückung unsicherer Bereiche.

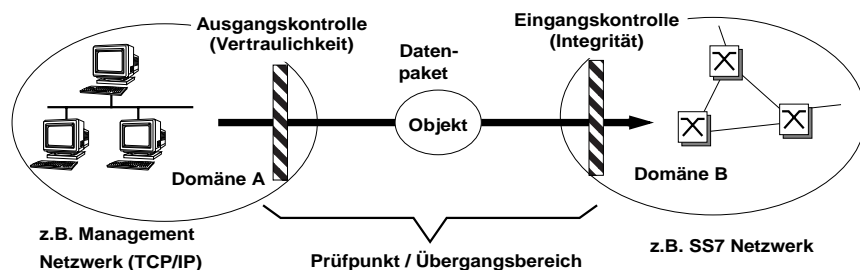


Bild 1: Übergang zwischen separat gesicherten Teilnetzen (Domänen)

Wir verwenden eingangsseitig Integritätsanforderungen und ausgangsseitig Vertraulichkeitsanforderungen als Prüfregeln an den Domänen-Übergängen:

- *Integrität*: Jeder Nachricht oder jedem Parameter kann eine Integritätsklasse zugeordnet werden. Die Integritätsklasse von Daten beschreibt die "Vertrauenswürdigkeit" dieser Daten im Hinblick auf ihre Verarbeitung durch sensitive Netz- oder Anwendungsfunktionen.
- *Vertraulichkeit*: Jeder Nachricht kann eine Vertraulichkeitsklasse zugeordnet werden. So klassifizierte Nachrichten werden nur in jene benachbarten Domänen entlassen, die eine entsprechende Berechtigung (Clearing) besitzen.

Die Ursprungs-Domäne A prüft vor dem Weiterleiten von Daten an eine angrenzende Domäne B, ob die Vertraulichkeitsklasse der Daten diese Weiterleitung über B an den Zielbereich erlaubt oder nicht. Ausgangsseitig wird folglich die Vertraulichkeitsanforderung vor der Freigabe geprüft. Eingangsseitig prüft Bereich B, ob die Integritätsklasse der Daten eine Verarbeitung innerhalb des Bereiches zuläßt. Dadurch wird Manipulationen der bereichsinternen Steuerung durch extern eingeschleuste manipulierte Steuerungsdaten entgegengewirkt. Dies entspricht einer Annahme-Prüfung. Die Vertraulichkeits- und Integritätsklasse einer Nachricht passen sich an die Sicherheitsklassen der von dieser Nachricht durchlaufenen Domänen (im Sinne einer Verschärfung der Schutzanforderungen) an.

2 Verwandte Arbeiten

Bell und LaPadula führen in [3] allgemeine Zugriffskontroll-Modelle ein. Denning erweitert in [1] dieses Modell durch geordnete Mengen (Lattices) zur Beschreibung von Vertraulichkeitsklassen und legt den Grundstein für Mandatory Access Control-Modelle [7]. Biba führte in [6] Integritätsklassen ein. Gemein ist den Verfahren, daß ein Monitor alle Zugriffe auf geschützte Objekte überwacht.

Bei Mandatory Access Control-Modellen kann der Besitzer eines Objektes die Zugriffsrechte jedoch nicht ändern. Allen Instanzen (Subjekten) sind Sicherheits-Clearings zugewiesen (z.B. Clearing für vertrauliche Daten); alle geschützten Objekte sind Sicherheitsklassen zugeordnet (z.B. streng vertraulich). Ein Zugriff über den Monitor wird erlaubt, falls das Clearing der zugreifenden Instanz mindestens der Vertraulichkeitsklasse entspricht, die dem Objekt zugeordnet ist. Sensible Anwendung (mit Integritäts-Clearing) dürfen entsprechend nur auf Daten mit derselben oder höherer Integritätsklasse arbeiten.

Das sogenannte High Water Mark-Modell (Weissman [4]) ermöglicht das dynamische Klassifizieren von Objekten. In [4] erhält eine Datei jeweils die Vertraulichkeitsklasse der Anwendung, die zuletzt auf diese Datei zugegriffen hat. Für Integritätsklassen gilt entsprechend, daß Daten die Integritätsklasse der Anwendung erben, die das letzte Mal schreibend darauf zugegriffen hat. Die Integrität von Daten wird dabei gewöhnlich herunterklassifiziert, die Vertraulichkeitsklasse nach oben verändert. Karger et. al. stellen in [5] ein Zugriffskontroll-Modell mit Vertraulichkeits- und Integritätsklassen für Chipkarten vor.

Wir wenden das Mandatory Access Control-Modell für Vertraulichkeits- und Integritätsklassen auf den Nachrichtenaustausch zwischen zusammengeschalteten Kom-

munikationsnetzen an. Sicherheits-Label (eingeführt für IP in [2]) kennzeichnen die Vertraulichkeits- und Integritätsklasse von Nachrichten. Zusätzliche Tags speichern Kontext-Information (Incoming Linkset, etc.) zur späteren Verarbeitung. Eine dynamische Anpassung der Sicherheitsklassen von Nachrichten wird an den Übergängen zwischen den Netzen vorgenommen. Sicherheitsaspekte der Zusammenschaltung offener Telekommunikationsnetze werden in [11] und [12] behandelt. Die Verwendung von Sicherheits-Labeln in Signalisiernetzen wurde in [8] vorgestellt. Steve Bellovin beschreibt in [9] ein Verfahren, bei dem Firewall-Funktionen bis in die Benutzer-Terminals verlegt werden. Wir verteilen die Filterfunktionen auf Netzgrenzen und zielen auf sichere Übergänge von Kommunikationsnetzen ab, nicht auf Benutzersicherheit.

3 Verteiltes Filtern

An jedem Übergangspunkt zwischen sicherheitstechnisch eigenständigen Teilnetzen (Domänen) muß entschieden werden, ob bestimmte Datenpakete die Netzgrenze passieren dürfen. Diese Zugriffssteuerung (Access Control) besteht aus Entscheidungsfunktionen (Access Control Decision Functions) und Durchsetzungsfunktionen (Access Control Enforcement Functions). Wir beschreiben im nächsten Abschnitt die Kriterien, die in Entscheidungsfunktionen verwendet werden und behandeln anschließend die allgemeine Struktur von Filtern und deren Verteilungsaspekt.

3.1 Sicherheits-Label und Contags

Sicherheits-Label und Contags speichern Informationen, auf deren Grundlage entschieden wird, ob Datenpakete in einen Bereich eingelassen oder aus einem Bereich entlassen werden. Sie sind die Eingangsgrößen für die Entscheidungsfunktion.

Sicherheits-Label speichern Sicherheitsklassen eines Datenpaketes im Datenpaket selbst. Wir unterscheiden Vertraulichkeit und Integrität. Die Zuordnung von Sicherheitsklassen zu Datenpaketen und Domänen ist Aufgabe der sogenannten Sicherheits-Policy eines Unternehmens. Bezüglich *Vertraulichkeit* und *Integrität* können folgende Sicherheitsklassen unterschieden werden, die bezüglich ihrer Indizes geordnet sind:

V0 nicht vertraulich

V1 vertraulich, Nutzdaten oder Netzsteuerdaten (z.B. zum Schutz vor der Erzeugung von Dienstnutzungsprofilen durch Dritte)

V2 streng vertraulich, z.B. Management-Passwörter zum Remote-Management

I0 keine Integrität garantiert, z.B. Benutzereingaben

I1 minimale Integrität, z.B. Benutzer initiierte Steuerdaten (Verbindungswunsch)

I2 mittlere Integrität, z.B. netzintern / von anderen Netzbetreibern erzeugte Daten

I3 hohe Integrität, z.B. Netzmanagementdaten (nur intern, z.B. SNMP², OMAP³)

Diese Klassen können anders gewählt werden, müssen aber an den Netzgrenzen von angrenzenden Bereichen konsistent interpretiert werden. Sicherheits-Label begleiten ein Datenpaket und können netzübergreifend verwendet werden.

2. SNMP: Simple Network Management Protocol

3. OMAP: Operation and Maintenance Application Part

Contags sind im Gegensatz zu Sicherheits-Labeln nur innerhalb einer Domäne von Bedeutung. Sie speichern Kontextinformation, die aus der Umgebung (Kommunikationskontext) abgeleitet wird. Beispiele für Kontextinformation sind Incoming Linkset/Network, Time of Arrival und Protection Level on Arrival (z.B. IPSec geschützt). Gewöhnlich ist diese Kontextinformation nur am Entstehungsort vorhanden und wird dort zum Filtern verwendet. Die sich bei unserem Verfahren durch Contags im Datenpaket ansammelnde Kontextinformation (Historie) kann zu einem späteren Zeitpunkt von einer Entscheidungsfunktion mit feinerer Granularität verwertet werden.

Aufgrund der Bedeutung, die Contags und Sicherheits-Label für die Entscheidungsfindung bei der Zugriffssteuerung haben, müssen sie beim Transport über unsichere Netzbereiche gegen Manipulation geschützt werden, beispielsweise durch Message Authentication Codes (kryptographisch gesicherte Nachrichten-Hashwerte). Zusätzlich werden in Entscheidungsfunktionen herkömmliche Datenpaket-Felder verwendet, beispielsweise die Ursprungs- oder Zieladresse oder der Datentyp einer Nachricht (Nutz-, Steuer- oder Management-Pakettyp, nationale Parameter).

3.2 Bausteine der Zugriffskontrolle an Netzübergängen

Aufbauend auf den Sicherheits-Labeln und Contags kann der Übergang zwischen Domänen mit Hilfe dreier aufeinander aufbauender Stufen beschrieben werden:

Eine *Eingangsprüfung* entscheidet, welchen Labels und Tags vertraut wird. Diese Entscheidung ist abhängig von der Sicherheits-Policy, die beschreibt welchen Netzbetreibern wieweit vertraut wird. Am Eingang muß die Integritätsklasse des Datenpaketes geprüft werden. Ist das Datenpaket P durch I(P) klassifiziert und ist die Domäne D der Klasse I(D) zugeordnet, so muß das Datenpaket in der Filterstufe (s.u., dritte Stufe) verworfen werden, falls $I(P) < I(D)$. Dies schützt sensible Anwendungen der Domäne vor manipulierten Daten. Diese Prüfung macht nur dann Sinn, wenn der Klassifizierungsinformation im Datenpaket vertraut wird. Eventuell vorhandene Message Authentication Codes oder Signaturen können hier geprüft werden, um Vertrauen in die Daten zu erzeugen. Kann dem Datenpaket nicht vertraut werden, so wird das Datenpaket als nicht authentisch markiert und in der zweiten Stufe pessimistisch mit neuen Sicherheits-Labeln versehen.

Die zweite Stufe ist für das *Context-Tagging* und für die *Label-Anpassung* zuständig. Neue Contags können dem Datenpaket hinzugefügt werden, beispielsweise als Secure Header Option [2] in IP-Paketen oder in freien Feldern von Signalisier Nachrichten des SS7. Außerdem werden die Sicherheitsklassen des Datenpaketes angepaßt. Besitzt die Domäne ein Clearing für die Vertraulichkeits-Klasse V(D) und ist ein Datenpaket P der Klasse V(P) zugeordnet, dann wird das Datenpaket neu klassifiziert und V(D) zugeordnet. $V(D) \geq V(P)$ gilt, da das Paket sonst am Ausgang der sendenden Domäne gefiltert worden wäre (s.u., Filter). Dieses Umklassifizieren ist notwendig, da Rechner innerhalb des Bereiches hoch klassifizierte Daten zum Datenpaket hinzufügen können. Ein nicht authentisiertes Datenpaket P mit Integritätsklasse I(P) aus der sendenden Domäne S mit I(S) erhält als neue Integritätsklasse $I(P) := \min(I(S), I(P))$. Die Default-Integritätsklassen umgebender Domänen sind von der Unternehmens-Policy festzulegen.

Eine dritte Stufe (*Filter*) filtert Datenpakete aufgrund der Tags und Label sowie sonstiger Paketinformation. Eine Domäne hat immer Ein- und Ausgangs-Filter, sofern Bereichsübergänge bidirektionalen Verkehr erlauben. Am Eingang werden Datenpakete mit Integritätsklasse $I(P)$ ausgefiltert (verworfen oder protokolliert), falls bzgl. der Integritätsklasse $I(D)$ der Domäne gilt: $I(D) > I(P)$, d.h. die Domäne eine höhere Datenintegrität fordert als das Paket anbietet. Am Ausgang werden Datenpakete ausgefiltert, deren Vertraulichkeitsklasse $V(D)$ größer ist als die Vertraulichkeitsklasse der Domäne, an die das Paket geschickt wird, d.h. falls die Daten zu sensibel sind.

3.3 Verteilte Filterung

Das von uns vorgeschlagene Filterverfahren kann aufgrund der Strukturierung und Hinzunahme von Tags verteilt implementiert werden. Heute vorhandene Filter integrieren gewöhnlich alle drei Filterstufen. Bild 2 zeigt links einen herkömmlichen Filter. Für Daten aus den Quellbereichen Q1 oder Q2 werden zunächst die für Zugriffsentscheidungen relevanten Eigenschaften festgestellt. Danach wird aufgrund von Entscheidungsregeln das zu übertragende Datum entweder weitergeleitet oder verworfen. Eine solche Architektur findet sich beispielsweise in Firewall-Routern oder in Betriebssystemkernen. Implizite Informationen, z.B. der Incoming Link, sind in späteren Filtern nicht mehr sichtbar.

Auf der rechten Bildhälfte ist das verteilte Filtern zu sehen. Die Prüffunktion befindet sich am Eingang einer Domäne. Filterfunktionen sind verteilt; Eingangsfiler und Ausgangsfiler können auf impliziten Informationen arbeiten, die in den Contags gespeichert sind..

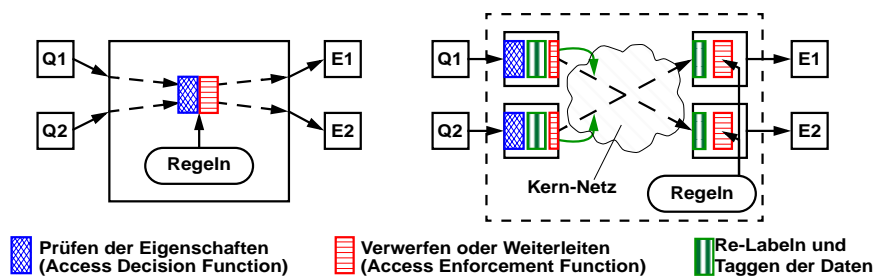


Bild 2: Übergang zu verteilter Filterung basierend auf Contags und Labeln

Die Prüfung der Eigenschaften findet direkt am Übergabepunkt der Daten statt. Nicht authentische Daten werden markiert. Danach wird das Re-Labeln entsprechend Stufe 2 in Abschnitt 3.2 durchgeführt. In der Eingangsstufe wird die Integrität geprüft (siehe Stufe 3 in Abschnitt 3.2). Datenpakete, die innerhalb des Bereiches verarbeitet werden könnten⁴, müssen hier gegebenenfalls verworfen werden. Vor der Ausgabe eines Datenpaketes an einen empfangenden Netzbereich (E1 oder E2) werden Vertraulichkeitsanforderungen geprüft und die Sicherheitsrichtlinien bezüglich der Klassifizierung

4. Dies ist der Fall, wenn die Zieladresse innerhalb des Bereiches liegt oder nicht vollständig bekannt ist; z.B. bei Global Title-Adressierung.

gen durchgesetzt. Daten, die innerhalb einer Domäne erzeugt werden, erhalten beim Re-Labeln vor dem Ausgangsfiltern automatisch die Vertraulichkeitsklasse und Integritätsklasse dieser Domäne.

Der Vorteil dieses Verfahrens ist, daß die Entscheidung über die Zulässigkeit eines Informationsflusses zu einem späteren Zeitpunkt auf Basis von kumulierter Kontextinformation (Historie) erfolgen kann, die ohne Sicherheits-Label und Contags nicht mehr sichtbar wäre. Da der Übergangsbereich (gestrichelte Linie) vertrauenswürdig sein muß, müssen auch die darin liegenden Kommunikationspfade hinsichtlich ihrer Integrität und gegebenenfalls hinsichtlich ihrer Vertraulichkeit geschützt werden.

3.4 Sicherheitstechnische Kompatibilität von benachbarten Domänen

Das oben eingeführte Re-Labeln von Datenpaketen führt gewöhnlich zu “überklassifizierten” Datenpaketen. Um die Kommunikation nicht unnötig einzuschränken, werden Maßnahmen berücksichtigt, die den Zugriff auf hoch klassifizierte Daten in niedrig klassifizierten Transitbereichen verhindern (z.B. Verschlüsselung).

Wir unterscheiden bei der Kompatibilität von benachbarten Domänen folglich zwei Fälle: Wenn Daten des sendenden Bereiches im benachbarten Bereich verarbeitet werden, dann müssen die in Abschnitt 3.2 eingeführten Regeln für Integritäts- und Vertraulichkeitsklassen streng eingehalten werden. Ist der benachbarte Bereich jedoch nur ein übermittelnder Bereich, so können additive Schutzmaßnahmen (Verschlüsselung bzw. Integritätsschutz z. B. mit Hilfe von IPSec-Tunneln) zur sicherheitstechnischen Überbrückung der Domäne genutzt werden. Die Prüfung der Sicherheitsklassen erfolgt dann basierend auf dem über den geschützten Tunnel verbundenen entfernten Bereich. Daraus folgt, daß nicht vertrauenswürdige Transfer-Bereiche

- nicht zur “Herunterklassifizierung” der Integrität von Datenpaketen (in der empfangenden Domäne) führen, sofern die Pakete über einen integritätsgeschützten Tunnel empfangen werden. Das Tunneln kann in Contags für die spätere Auswertung gespeichert werden. Das Re-Labeln der Eingangsstufe berücksichtigt diese Tags beim Bestimmen der Integritätsklasse eines empfangenen Paketes.
- vertrauliche Daten übertragen können, wenn diese Daten über einen vertraulichkeitsschützenden Tunnel übertragen werden. Dieses wird beim Re-Labeln am Ausgang des Sendebereiches berücksichtigt. Nach dem Verschlüsseln wird die Vertraulichkeitsklasse *V0* in das umschließende Datenpaket geschrieben, so daß der Ausgangsfilter die Daten in den nicht vertrauenswürdigen Bereich senden kann.

Ob geschützte Kanäle verwendet werden, wird bei zentralen Policy-Datenbanken oder – beim Verwenden von IPSec – direkt bei der IPSec Policy-Datenbasis abgefragt.

3.5 Anwendungsbeispiel

Als Beispiel für den Einsatz verteilter Filterung mit Contags wird die Zusammenschaltung von ISDN-Signalisiernetzen mehrerer Betreiber (A, B und C) betrachtet. Ein Zwischensignalisiernetz ZSN unter der Kontrolle von Betreiber A verbindet die Netze A, B und C. Die erlaubten Verkehrsarten zwischen den Netzen sind durch Verträge zwischen den Netzbetreibern festgelegt. A akzeptiert von B und C jegliche ISUP-Signalisier Nachrichten zur Rufsteuerung⁵. Jedoch soll nur B auf höherwertige Netz-

dienste (z.B. Dienste des Intelligenten Netzes) zugreifen dürfen; das ZSN erlaubt den Austausch von Signalisier Nachrichten zur Steuerung höherwertiger Dienste (z.B. IN Dienste) nur zwischen B und A.

Eine Auswertung von Informationen höherer Protokollschichten (z.B. SS7-Anwender Teile wie Intelligent Network Application Protocol, INAP) ist am Zugangspunkt zum ZSN wegen des hohen protokolltechnischen Aufwandes jedoch nicht praktikabel (Performance-Verlust). Beim Filtern am Übergang zum Zielnetz kann der Absender aber nicht zweifelsfrei festgestellt werden, da die Korrektheit der Absenderadresse (Origination Point Code, OPC) zu diesem Zeitpunkt (ohne Contags) nicht mehr überprüft werden kann.

Daher wenden wir hier verteiltes Filtern mit Sicherheits-Labeln und Contags an. Wir prüfen die Authentizität der Absenderadresse einer Nachricht schon am Eingang des ZSN und vermerken das Prüfergebnis anhand eines Contags in der Signalisier Nachricht. Bei den betrachteten Nachrichten handelt es sich um Schicht 3-Nachrichten des SS7 (Message Transfer Part-Nachrichten). Sicherheits-Label und Tags werden auf "Sparebits" des Service Indicator Octets der MTP-Nachrichten abgebildet, wie in Bild 3 dargestellt [13].

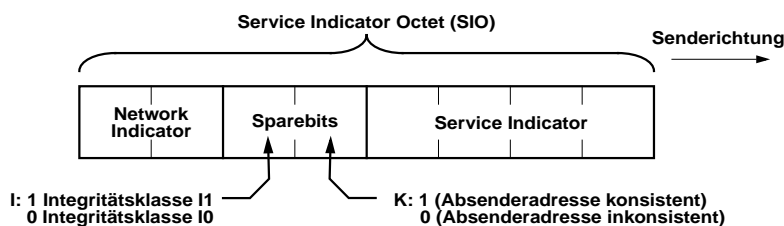


Bild 3: Nutzung des Service Indicator Oktets für Contags

Zunächst wird Netz A logisch in zwei Teilnetze A1 und A2 zerlegt, die über eigene Zugangspunkte mit dem ZSN verbunden werden (vgl. Bild 4). Während der Zugangspunkt A1 nur ISUP-Verkehr behandelt (Service Indicator SI=5) wird der übrige Verkehr über den Zugangspunkt A2 geführt. Den Netzen B und C werden unterschiedliche Integritätsklassen (I0 und I1) zugeordnet.

Bei Entgegennahme einer Nachricht durch das ZSN wird zunächst die Korrektheit der Absenderadresse (OPC) bezüglich des Incoming Link geprüft und als Contag im Adress-Header der Nachricht vermerkt (K=1: konsistent). Sofortiges Ausfiltern der Nachrichten ist nicht möglich, da bezüglich des Verkehrs zwischen B und C unter Umständen andere Anforderungen hinsichtlich zulässiger OPCs bestehen⁶. Die Integritätsklasse des Ursprungsnetzes wird durch ein Integritäts-Label I in der MTP-Nach-

5. Der ISDN User Part (ISUP) unterstützt die Steuerung der leitungsgebundenen Kommunikation im digitalen Telefonnetz. Dies geschieht über Signalisier Nachrichten, die über den Message Transfer Part (MTP), ein paketvermittelndes Netz, ausgetauscht werden.

6. Dieser Fall kann beispielsweise auftreten, wenn das ZSN eine Transitfunktionalität (Signalling Transfer Point, STP) für Signalisierverkehr zwischen B und C bereitstellt.

5 Literatur

- [1] D. E. Denning: A Lattice Model of Secure Information Flow. *Communications of the ACM*, Vol. 19, No. 5, May 1976, pp. 236-243.
- [2] S. Kent: Security Options for the Internet Protocol. Nov 1991. RFC 1108.
- [3] D. E. Bell, L. J. LaPadula: Computer Security Model Unified Exposition and Multics Interpretation, The MITRE Corp., ESD-TR-75-306, Ma., June 1975. (NTIS # AD A023588)
- [4] C. Weissman: Security Controls in the ADEPT-50 Time Sharing System. 1969 Fall Joint Computer Conference, AFIPS, Vol 35, AFIPS Press, Montvale, N. J., 1969, pp. 119-133.
- [5] P. A. Karger, V. R. Austel, D. C. Toll: Using a Mandatory Secrecy and Integrity Policy on Smart Cards and Mobile Devices. EUROSMART Security Conference, June 2000.
- [6] K. J. Biba: Integrity Considerations for Secure Computer Systems. ESD-TR-76-732, HQ Electronic Systems Division, Hanscom AFB, Ma., April 1977.
- [7] R. S. Sandhu: Lattice-Based Access Control Models. *IEEE Computer*, Vol. 26, No. 11, November 1993, pages 9-19.
- [8] M. Kabatnik, R. Sailer: Modelling of Secure Interconnection. Communication Fraud Control Association, 1999 Spring International Conference in Ismaning/Germany, May 1999.
- [9] S. Bellovin: Distributed Firewalls. *login*, Nov 1999, pp. 37-39.
URL: <http://www.research.att.com/~smb/papers/distfw.pdf>
- [10] Sailer, R., Kühn, P.: Ein Domain-Konzept zur systematischen und wirtschaftlichen Integration von Sicherheit in Kommunikationsnetzen. *Informationstechnik und Technische Informatik*. Bd. 38 (1996) Heft 4, S. 30-33.
- [11] K. Ward: The Impact of Network Interconnection on Network Integrity. *British Telecommunications Engineering*, Vol. 13, January, 1995.
- [12] Sailer, R.: Security Services in an Open Service Environment. Proc. 14th ACSAC, Phoenix, Arizona, IEEE Computer Society, Los Alamitos, pp. 223-234.
- [13] ITU-T Recommendation Q.704: Specification of Signalling System No. 7 — Message transfer part — Signalling network functions and messages; ITU, 1996.