in: Günter Müller, Andreas Pfitzmann (Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik, Addison-Wesley-Longman 1997, 325-357.

15

Allokation von Sicherheitsfunktionen in Telekommunikationsnetzen

R. Sailer[1], H. Federrath[2], A. Jerichow[2], D. Kesdogan[3], A. Pfitzmann[2]

Ein Kommunikationsnetz ohne Sicherheitsfunktionen ist heute undenkbar. Sicherheit umfaßt die Erfüllung der Anforderungen Vertraulichkeit (confidentiality), Integrität (integrity) und Verfügbarkeit (availability) in einem Rechnernetz. Telekommunikationsnetze sind heutzutage ebenfalls Rechnernetze, auf denen verteilte Anwendungen implementiert sind. In solchen Netzen fallen an vielen Stellen schützenswerte Daten in erheblichem Umfang an. Neben Verbindungsdaten und Abrechnungsdaten sind dies natürlich die Inhalte der Kommunikation.

Neben der Integration von Konzepten zur Datenvermeidung ist die Sicherung der vorhandenen und notwendigen Daten erforderlich. Diese Aufgabe wird durch sog. Sicherheitsmechanismen erfüllt. Die Anordnung (Allokation) dieser Sicherheitsmechanismen entscheidet einerseits über die Wirksamkeit der Sicherheitsfunktionen, andererseits beeinflußt sie die Leistungsparameter des Netzes. Daher ist die geschickte Anordnung der Sicherheitsmechanismen eine notwendige Voraussetzung für die Akzeptanz von Sicherheit.

1 Universität Stuttgart, Institut für Nachrichtenvermittlung und Datenverarbeitung, Email: sailer@ind.uni-stuttgart.de

2 TU Dresden, Institut für Theoretische Informatik, Email: {federrath, jerichow, pfitza}@inf.tu-dresden.de

3 RWTH Aachen, Lehrstuhl für Informatik IV, Email: dogan@i4.informatik.rwth-aachen.de

Dieses Papier betrachtet verschiedene Möglichkeiten der Allokation von Sicherheitsfunktionen, ohne auf ihre innere Struktur selbst einzugehen. Sie können als eine Art Black-Box betrachtet werden.

15.1 Klassifikation von Funktionen in Telekommunikationsnetzen

Funktionen in Kommunikationsnetzen lassen sich entsprechend der Möglichkeit ihrer Anordnung innerhalb verschiedener Netzknoten und Schichten klassifizieren. Als Grundlage der Klassifikation werden die Beziehungen zwischen den Instanzen, welche die verteilte Funktionalität erbringen, sowie die Instanzen selbst festgelegt.

Dies entspricht zwei grundsätzlichen Freiheitsgraden zur Allokation:

- Horizontaler Freiheitsgrad entlang der Komponenten (Knoten) eines Kommunikationsnetzes und
- Vertikaler Freiheitsgrad entlang der Schichten eines Kommunikationsnetzes.

Abb. 15.1 illustriert diese beiden Freiheitsgrade am Beispiel der Funktionsverteilung im Teilnehmeranschlußbereich eines Telefonnetzes.

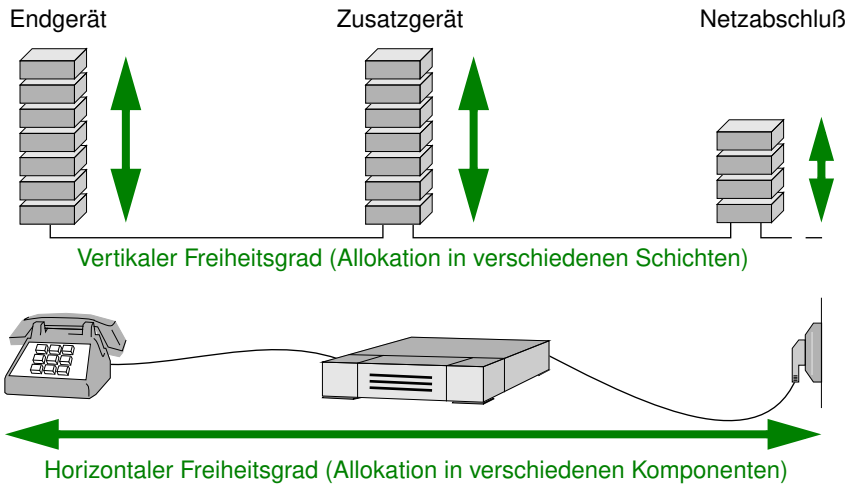


Abbildung 15.1: Beispiel der Freiheitsgrade bei der Allokation von Funktionen im Teilnehmeranschlußbereich eines Telefonnetzes

Wir wollen Funktionen in Kommunikationsnetzen folgendermaßen unterteilen:

- Eine Funktion wird Link-zu-Link (LzL) genannt, falls sie durch zwei benachbarte Knoten des Kommunikationsnetzes erbracht wird und sich auf einen festen physischen Übertragungsabschnitt (Link) bezieht.
- Eine Funktion wird Knoten-zu-Knoten (KzK) genannt, wenn zwischen den die Funktion erbringenden Knoten weitere Knoten im Kommunikationsweg existieren. Der dazwischen liegende Teil des Kommunikationsnetzes wird dabei nur als Transportmedium genutzt und ist nicht an der Realisierung der Funktion beteiligt.
- Eine Funktion wird Ende-zu-Ende (EzE) genannt, wenn sie die Endpunkte einer Kommunikationsbeziehung betrifft. Alle dazwischen liegenden Teile des Kommunikationsnetzes sind nicht an der Realisierung der EzE-Funktion beteiligt und werden nur als Transportmedium genutzt.

Diese Begriffsbestimmungen zeigen, daß EzE und LzL Grenzfälle sind.

EzE-Sicherheit kann folgendermaßen abgeleitet werden: EzE-Sicherheit ist die Erfüllung der Sicherheitsanforderungen bezüglich der Kommunikationsbeziehung zwischen zwei (oder mehreren) Instanzen durch EzE-Funktionalität. Analog kann LzL-Sicherheit und KzK-Sicherheit definiert werden.

Voydock und Kent [VoKe_83] unterscheiden nur nach EzE und LzL und wenden entsprechende Sicherheitsfunktionen in folgender Weise an: LzL-orientierte Schutzmaßnahmen bieten Sicherheit für Informationen, die über eine individuelle Übertragungsleitung zwischen zwei Knoten übertragen werden ohne Beachtung der ursprünglichen Quelle bzw. Senke dieser Informationen. EzE-orientierte Sicherheitsfunktionen dagegen modellieren ein Netzwerk als Transportmedium, um die Protocol Data Units (PDUs) in einer sicheren Weise von der Quelle zur Senke zu transportieren. EzE-Sicherheitsmaßnahmen schützen PDUs bei der Übertragung zwischen den Endpunkten einer Kommunikationsbeziehung, so daß Angriffe an den Übertragungsabschnitten die Vertraulichkeit und Integrität der transportierten Information nicht beeinträchtigen können.

Die folgenden Beispiele sollen die Anwendung der Begriffe auf Sicherheitsanforderungen verdeutlichen. A bezeichnet den rufenden und B den gerufenen Teilnehmer innerhalb einer Kommunikationsbeziehung.

- *EzE-Vertraulichkeit/Integrität des Kommunikationsinhaltes:* A und B kommunizieren miteinander und sind alleine dafür verantwortlich, daß die Vertraulichkeit bzw. Integrität des Kommunikationsinhaltes gewahrt wird. Dazu fügen A und B Sicherheitsfunktionen in ihren Endgeräten ein.
- *EzE-Verfügbarkeit eines Dienstes:* A und eine Datenbank kommunizieren miteinander und sind alleine dafür verantwortlich, daß zu einer beliebigen Zeit

eine Anfrage von A durch die Datenbank innerhalb einer Zeit Δt beantwortet wird (Verfügbarkeit des Netzes als Voraussetzung für Anfragen bzw. Antworten). Die Datenbank muß dazu die verschiedenen Anfragen den zugreifenden Instanzen sicher zuordnen können, um eine vorsätzliche Überlastung der Datenbank durch Dritte zu verhindern (Fairness). Die Sicherheitsfunktionen sind in den Endgeräten und der Datenbank plaziert.

- *LzL-Sicherung gegen Übertragungsfehler zwischen Teilnehmerstation und erstem Vermittlungsknoten*: Die Sicherung gegen Übertragungsfehler zwischen einer Teilnehmerstation und dem ersten Vermittlungsknoten im Netz ist eine LzL-Funktion, die z.B. mit Hilfe von High-Level-Data-Link-Control-Protokollen (HDLC) realisiert wird.
- *KzK-Sicherung gegen Übertragungsfehler zwischen Netzübergängen:* Eine Fehlersicherung zwischen Netzübergängen ist eine KzK-Funktion, da sie übergreifend über das zwischenliegende Kommunikationsnetz erfolgt und i.a. verschiedene Links überspannt.
- *EzE-Fehlersicherung auf der Anwendungsebene:* Eine Fehlersicherung auf Anwendungsebene ist eine EzE-Funktion, da sie über verschiedene Netzknoten hinweg bzw. nicht auf einen Übertragungsabschnitt wirkt und innerhalb der übergeordneten Endpunkte der Kommunikationsbeziehung realisiert ist (z.B. in Endgeräten).

Abb. 15.2 zeigt LzL-, KzK- und EzE-Funktionen zwischen verschiedenen Netzknoten. Der Übergang von LzL-Funktionen zu KzK-Funktionen findet mit dem Überspringen von dazwischen liegenden Netzknoten statt. Das Bild zeigt ebenfalls die EzE-Beziehung zwischen den Endgeräten (Knoten A und B). Die dazwischen liegenden Knoten symbolisieren Netzknoten oder auch Zusatzgeräte im Teilnehmerbereich (z.B. Telekommunikationsanlagen). Bezüglich zweier oder mehrerer Netzknoten lassen sich Grenzen für die Realisierung von LzL-, KzK- bzw. EzE-Funktionen definieren.

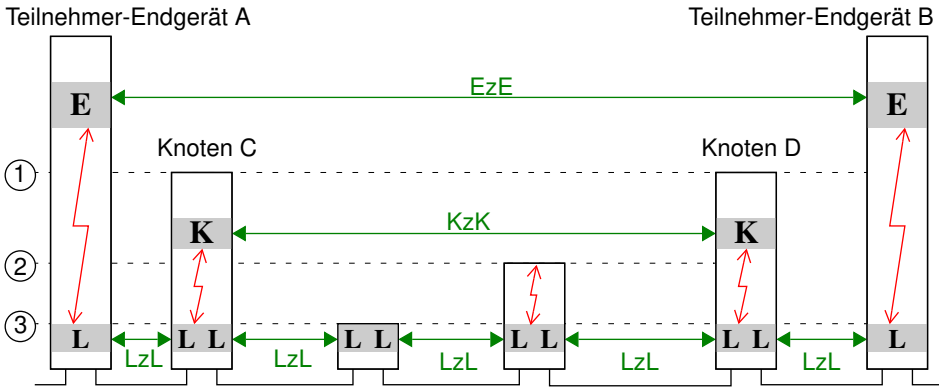
Die *EzE-Grenzlinie* beschreibt die untere Grenze für die Realisierung von EzE-Funktionalität. Beispielsweise können Vermittlungsdaten nicht innerhalb der Teilnehmerstationen EzE verschlüsselt werden, da die Netzknoten diese z. B. zur Verkehrslenkung verarbeiten müssen.

Innerhalb von paketvermittelten Netzen (verbindungslose Dienste) liegt die EzE Grenzlinie zwischen Schicht 3 und 4. Bei verbindungsorientierten Diensten (z.B. ISDN) liegt diese Grenzlinie innerhalb der Signalisierung zwischen Schicht 3 und 4, innerhalb der Nutzdatenprotokolle zwischen Schicht 1 und 2.

Diese Randbedingung garantiert, daß Funktionen darunterliegender Schichten durch die EzE-Sicherungsfunktion nicht beeinflußt werden.

Die *KzK-Grenzlinie* beschreibt die untere Grenze für die Realisierung von KzK-Funktionalität. Die KzK-Grenzlinie kann deutlich unterhalb der EzE-Grenzlinie liegen, da die Bezugspunkte im Verbindungsweg, zwischen denen die KzK-Funktionalität transparent erbracht werden muß, nicht mit den Endpunkten der übergeordneten Kommunikationsbeziehung übereinstimmen müssen (siehe Abb. 15.2). Knoten im Verbindungsweg zwischen Teilnehmer A und B, welche Funktionen hoher Schichten realisieren und deshalb die EzE-Grenzlinie nach oben verschieben, beeinflussen die Lage der KzK-Grenzlinie nur dann, wenn sie auch im Verbindungsweg zwischen den Knoten liegen, welche die KzK-Funktion realisieren.

Die *LzL-Grenzlinie* beschreibt die obere Grenze für die Realisierung von LzL-Sicherheitsfunktionen. Sie liegt am oberen Rand der höchsten Schicht, die von allen benachbarten Netzknoten implementiert ist. Benachbarte Netzknoten müssen an gemeinsamen Übertragungsabschnitten auf derselben Schicht jeweils duale Sicherheitsfunktionen realisieren.



① untere Grenze für EzE-Funktionen bezüglich A und B (EzE-Grenzlinie)
② untere Grenze für KzK-Funktionen bezüglich C und D (KzK-Grenzlinie)
③ obere Grenze für *einheitliche* LzL-Funktionen im dargestellten Netzausschnitt (LzL-Grenzlinie)

E EzE-Funktion
K KzK-Funktion
L LzL-Funktion

innerhalb von Knoten nicht durch Sicherheitsfunktionen geschützter Bereich (Gap)

Abbildung 15.2: EzE-, KzK- und LzL-Funktionen auf verschiedenen Betrachtungsebenen

Gaps bezeichnen Bereiche, die nicht durch die Sicherheitsfunktionen geschützt sind. So sind beispielsweise alle Protokollinformationen, die zwischen A und B unterhalb der EzE-Funktion und oberhalb der LzL-Funktion ausgetauscht werden, vor den Knoten C und D ungeschützt. Liegt innerhalb des Gaps in Endgerät A in Abb. 15.2 die Funktionalität zur Adressierung (Schicht 3), so kann die Netzadresse des Absenders bzw. des Adressaten innerhalb eines zwischenliegenden Knotens oberhalb der LzL-Sicherung beliebig manipuliert werden, ohne daß dies durch die EzE- oder LzL-Sicherungsfunktionen erkannt werden kann.

15.2 EzE- versus LzL-Sicherheitsfunktionen

Die Nutzer eines Kommunikationsnetzes wünschen sich eine EzE garantierte Dienstqualität, nicht nur bezüglich Vertraulichkeit und Integrität, sondern auch bezüglich der Verfügbarkeit. Mit Hilfe von EzE-Sicherheitsmechanismen ist Vertraulichkeit, teilweise auch Integrität, meist sehr gut realisierbar, während für die Sicherstellung von Verfügbarkeitseigenschaften unterstützende Maßnahmen des Netzes (z.B. redundante Auslegung der Netzknoten, Ersatzwege) erforderlich sind. Die folgenden Abschnitte versuchen, die Vor- und Nachteile sowie Wechselwirkungen der jeweiligen Allokationsformen herauszuarbeiten.

EzE-Sicherheitsfunktionen

Saltzer, Reed und Clark empfehlen in [SaRe_84], möglichst viel Funktionalität an den Endpunkten einer Kommunikation zu plazieren, d.h. die Nutzung von EzE-Funktionalität in dem Nutzer möglichst naheliegenden Schichten bzw. innerhalb der Anwendung. Sie definieren eine EzE-Beziehung als das Zusammenspiel von Funktionen an den Endpunkten des Kommunikationssystems. Sie sprechen sich insgesamt gegen die Realisierung von anwendungsunterstützender Funktionalität in niederen Schichten aus, weil die Funktionalität nur bis zu der Schicht wirkt, in der sie realisiert ist. Innerhalb von Zwischenknoten im Netz muß auf die korrekte Realisierung der oberhalb der Sicherheitsfunktion erbrachten Funktionen vertraut werden.

Praxisbeispiel Fehlersicherung [SaRe_84]: Mehrere Lokale Netze sind über Gateways verbunden. Zwischen den Gateways werden Checksummen zur Fehlersicherung verwendet unter der Annahme, daß die Hauptgefahr für Veränderungen auf den Übertragungsabschnitten liegt. Anwendungsprogrammierer verlassen sich dann auf die sogenannte „gesicherte Übertragung“, ohne zu beachten, daß die Daten innerhalb der Gateways (oberhalb der Sicherungsschicht) ungeschützt sind. Tatsächlich wurden in diesem ungesicherten Teil des Gateways durch transiente Fehler beim Kopieren von Daten zwischen Eingangs- und Ausgangspuffern Daten verändert. Über eine gewisse Zeit wurden auf diese Weise viele Quellcode-Dateien eines Betriebssystems (unerkannt) falsch

hin und her übertragen. Die ursprünglichen - fehlerfreien - Dateien mußten mit Hilfe von Papierausdrucken wiederhergestellt werden.

Auch innerhalb der Endpunkte der Kommunikation muß auf die korrekte Realisierung der Funktionen zwischen der Informationsquelle und der Realisierung der Funktionalität vertraut werden (siehe Gaps in den Endgeräten A und B in Abb. 15.2).

Darüber hinaus kann die Realisierung von EzE-Funktionalität die Komplexität der niedrigeren Schichten bedeutend verringern, wenn in jeder Schicht nur die notwendigen Funktionen realisiert werden. Dieses erhöht auch die Leistungsfähigkeit dieser Schichten. Ein weiterer Vorteil ist die „Selbstrealisierbarkeit" der Sicherheitsfunktionalität. Es bedarf normalerweise keiner Änderung der dazwischenliegenden Netzfunktionalität. Jeder Nutzer kann selbstkontrollierbar und selbstkonfigurierbar seine Endgeräte um Sicherheitsfunktionen erweitern. Dieses Vorgehen wirkt sich allerdings nachteilig auf die individuellen Kosten für den Teilnehmer aus, reduziert die Kompatibilität und eventuell auch die Interoperabilität zu anderen Teilnehmern. Außerdem könnte die freie Gestaltung selbstwählbarer Sicherheitsfunktionen durch organisatorische Rahmenbedingungen, z.B. Gesetzesauflagen für die Kryptographieverwendung, eingeschränkt sein.

LzL-Sicherheitsfunktionen

Die ausschließliche Verwendung von teilnehmerbestimmten EzE-Sicherheitsfunktionen trägt nicht dazu bei, einen Grundschutz z.B. gegen Outsider (externe Angreifer, etwa Abhörer auf einer Übertragungsleitung) zu gewährleisten. Dieser ist jedoch durch Einsatz von LzL-Sicherungsmaßnahmen realisierbar, auch wenn ein Teilnehmer auf eine EzE-Sicherung verzichten würde. Durch die gemeinsame Nutzung von LzL-Funktionen durch darüberliegende Funktionen ist eine effiziente Nutzung der Ressourcen möglich. Weiterhin sind die Protokollinformationen der höheren Schichten geschützt. So wird beispielsweise Adreßinformation vor einem Outsider verborgen. LzL-Sicherheitsmechanismen sind fehlertoleranter bei lokalen Störungen. So ist beispielsweise innerhalb der Protokolle der Zwischenamtssignalisierung eine alternative Wegewahl zum nächsten Link effizient möglich, falls Störungen auftreten. In einem Mix-Netz [Chau_81] dagegen sind bestimmte Knoten vom Benutzer bestimmbar vorgegeben. Das Mix-Netz schützt die Kommunikationsbeziehungen zwischen Sendern und Empfängern. Ist einer der gewählten Knoten gestört, kann er nur mit sehr hohem Aufwand „übergangen" werden [Pfit_90]. Andererseits erfordern LzL-Maßnahmen Vertrauen in die Knoten, welche die Funktionalität erbringen, da innerhalb des Knotens die Daten ungeschützt vorliegen.

Vereinigung der Vorteile von EzE- und LzL-Mechanismen

Es bietet sich eine Kombination von EzE- und LzL-Maßnahmen an, um die Vorteile beider Allokationsmöglichkeiten miteinander zu vereinigen. Wie dies geschieht, hängt stark von den Sicherheitswünschen und -anforderungen der Teilnehmer ab. Er muß einen optimalen Weg zwischen Kosten, Sicherheitswünschen und technisch realisierbaren beziehungsweise verfügbaren Sicherheitsfunktionen finden.

Beispielsweise könnte LzL-Verschlüsselung standardmäßig eingesetzt werden. Dies schützt nicht nur die Nutzdaten und Verkehrsdaten der Teilnehmer vor Outsidern, sondern beispielsweise auch Daten für Administration und Management des Betreibers der Links (Vermittlungsstellen, Datenbanken etc.). Über diesen Grundschutz hinaus kann sich der Nutzer auch gegen die Betreiber der Netze schützen, indem er EzE-Sicherheitsmaßnahmen ergreift, z.B. EzE-Verschlüsselung. Das Netz muß hierzu in jedem Fall die EzE-Sicherheitsmaßnahmen unterstützen bzw. ermöglichen. Leider ist das nicht in allen Netzen der Fall. In Mobilfunknetzen nach dem GSM Standard [GSM1_93] ist eine Verlängerung der GSM-Sprachkanäle zum ISDN hin nicht möglich, da die im GSM verwendete Sprachkomprimierung [GSM2_89, GSM3_92] nicht verlustfrei und damit bittransparent arbeitet. Folglich läßt sich die EzE-Verschlüsselung von Sprachinformation gar nicht oder nur auf Umwegen erreichen [Muel_96].

15.3 Grundmodell für die Allokation von Sicherheitsmechanismen

Sicherheitsfunktionalität kann grundsätzlich durch *Einfügen* möglichst *transparenter Zwischenschichten* in die Protokolltürme der Kommunikationsknoten oder durch Integration in die Anwendung selbst erfolgen.

Zusätzlich können *organisatorische Maßnahmen* und Vorschriften für die Nutzung und Bedienung von Anwendungen sowie Zugriffs- und Zugangskontrollen für Systemteile die Sicherheit eines Systems erhöhen. Auf diesen Aspekt wird jedoch im weiteren nicht näher eingegangen.

Allokationsgrenzen für LzL- und EzE-Sicherheitsmechanismen

Abb. 15.3 zeigt ein Grundmodell zur Allokation von Sicherheitsfunktionalität. Gleichzeitig ist es auch für die Beschreibung des Angreifermodells geeignet. Der Vertrauensbereich beschreibt, welchen Komponenten eines Systems vertraut wird. Dabei beinhaltet ein Vertrauensbereich implizit das Vertrauen in die korrekte Implementierung von Software bzw. fehlerfreie Hardware, und es werden dort keine Angreifer angenommen [Pfit_95]. Er ist immer einem be-

stimmten Anwender (bzw. Anwenderpaar bei einer Punkt-zu-Punkt-Verbindung oder einer Menge von Anwendern bei einer Punkt-zu-Multipunkt-Verbindung) zugeordnet, der in der jeweiligen Situation entscheidet, ob eventuell verbleibende Angriffsmöglichkeiten – in Verbindung mit dem für einen erfolgreichen Angriff erwarteten Aufwand – tolerierbar sind, oder ob zusätzliche Sicherheitsmaßnahmen ergriffen werden müssen.

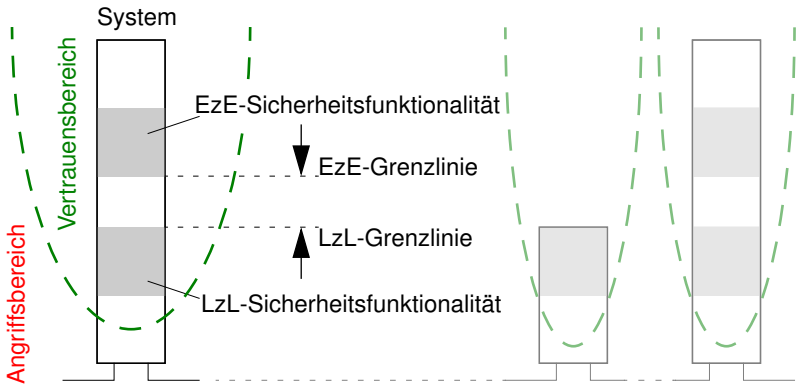


Abbildung 15.3: Grundmodell für die Allokation von Sicherheitsfunktionen

In die zwischen der EzE-Grenzlinie und der LzL-Grenzlinie liegenden Schichten kann aus folgenden Gründen i.a. weder EzE- noch LzL-Sicherheitsfunktionalität integriert werden:

- EzE-Sicherheitsfunktionalität kann nicht integriert werden, da mindestens ein Zwischenknoten die dadurch geschützten Daten verarbeiten müßte.
- LzL-Sicherheitsfunktionalität kann nicht installiert werden, da mindestens ein Nachbarknoten existiert, der in dieser Schicht die duale Sicherheitsfunktionalität nicht realisieren kann.

Innerhalb eines Knotens LzL-Sicherheitsfunktionalität auf verschiedenen Ebenen zu realisieren würde bedeuten, das gesamte Sicherheitsmanagement zu vervielfachen und von der Wegewahl abhängig zu machen, was aus Aufwandsgründen nicht empfehlenswert ist. Dieses Argument läßt sich auf die LzL-Sicherheitsfunktionsallokation des gesamten zu sichernden Netzbereiches erweitern. Folglich werden innerhalb eines Netzbereiches LzL-Sicherheitsfunktionen häufig auf der gleichen Schicht realisiert, was die LzL-Grenzlinie für praktische Anwendungen nach unten verschieben kann. In Netzübergängen kann eine Umsetzung von LzL-Funktionen auf verschiedenen Schichten realisiert werden.

Dies ist beispielsweise innerhalb des Anwendungsprotokollturms an der Schnittstelle von leitungsvermittelten (Funktionen der Schicht 1 implementiert) zu paketvermittelten Netzen (Funktionen der Schichten 1-3 implementiert) sinnvoll. Innerhalb des Teilnehmerbereiches können Sicherungen benachbarter Komponenten durchaus auf verschiedenen Ebenen realisiert werden, falls die Komponenten statisch verbunden sind. In solchen Fällen gestaltet sich das Sicherheitsmanagement besonders einfach.

Angreifermodell

Ein Angreifermodell beschreibt Angreifer mit ihren Angriffsmöglichkeiten, die für ein zu sicherndes System angenommen werden. Als System werden zwei Teilnehmerbereiche (Informationsquelle bzw. Informationssenke) betrachtet, die über ein Vermittlungsnetz gekoppelt sind.

Abb. 15.4 stellt mögliche Angriffspunkte innerhalb eines Systems dar, wobei ein Bezugspunkt durch die Informationsquelle bzw. Informationssenke auf Anwendungsebene gegeben ist. Zu diesen in der Anwendung erzeugten Daten werden bei der Protokollabarbeitung Protokolldaten (Steuerinformation) hinzugefügt. Außerdem können Informationen aus der Nutzung von Kommunikationsdiensten mit Hilfe einer Verkehrsflußanalyse gewonnen werden.

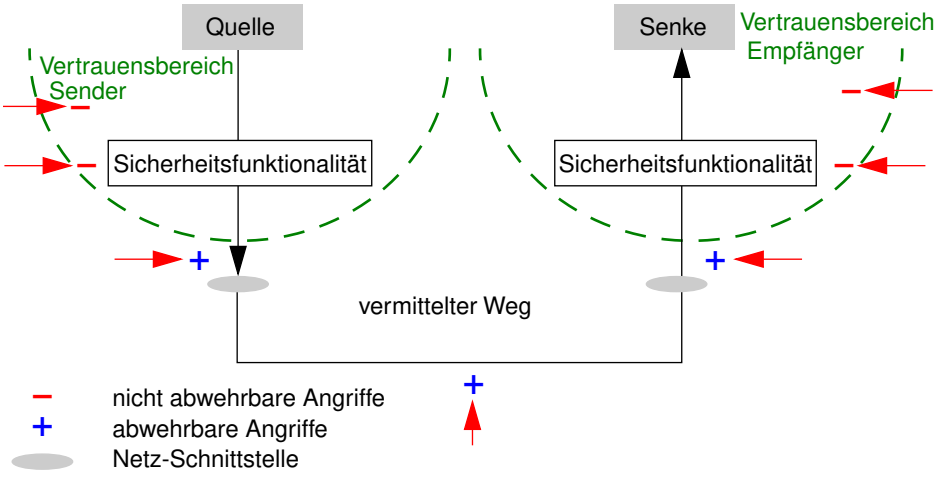


Abbildung 15.4: Angreifermodell für Telekommunikationsanwendungen

Besitzt der Angreifer Angriffspunkte zwischen der Quelle und der Sicherheitsfunktionalität oder entsprechend zwischen der Sicherheitsfunktionalität und

der Senke, so ist kein Schutz der Information gegeben, da die Informationsträger ungeschützt vorliegen. Deshalb muß zwischen der Quelle von zu schützenden Daten und der zum Schutz dieser Daten vorgesehenen Sicherheitsfunktionalität ein *sicherer Pfad* (*Trusted Path*) existieren, d.h. ein Weg, auf dem die Sicherheit der Informationsträger garantiert ist. Besitzt der Angreifer Angriffsmöglichkeiten bezüglich der Sicherheitsfunktionalität, so ist diese ohne Nutzen und kann bei Sicherheitsbetrachtungen nicht mit einbezogen werden [LaAh_86].

Agiert der Angreifer zwischen Sicherheitsfunktionalität und Netzschnittstelle (z.B. Abhören von Übertragungsmedien innerhalb des Teilnehmerbereiches), so sind alle Informationen, die ihren Ursprung oberhalb der Sicherheitsschicht haben, gesichert (je nach Sicherheitsfunktionalität gegen Kenntnisnahme und/ oder unerkannte und unautorisierte Veränderung).

Angriffe innerhalb des vermittelnden Netzes (Anschlußleitung, Zwischenamtsleitung) und auf Empfängerseite zwischen der Netzsschnittstelle und der Sicherheitsfunktionalität sind äquivalent. Die im Rahmen der Protokollabarbeitung unterhalb der Sicherheitsfunktionalität hinzugefügte Information (z.B. Adressen, Dienstkennungen, Menge der Daten, Richtung, Zeitstempel, Kommunikationsverhalten) ist ungeschützt und kann – ohne entsprechende Gegenmaßnahmen – von Angreifern unerkannt geändert bzw. ausgespäht werden (Abb. 15.5).

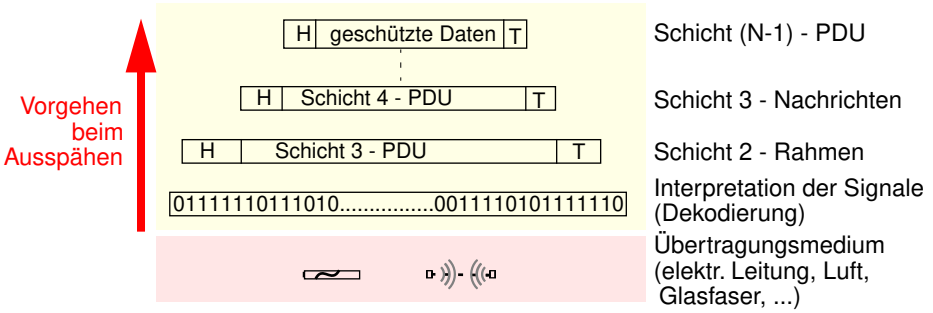


Abbildung 15.5: Angriff durch Abhören des Übertragungsmediums

In einem ersten Schritt werden die abgehörten Signale dekodiert (Kanaldekodierung und Umkehr der Quellkodierung). Dabei erhält der Angreifer die Schicht 2-Rahmen und die dazugehörige Protokollinformation (H für Header, T für Trailer) im Klartext. Die dazwischenliegende Schicht 3-PDU kann ebenso ausgepackt werden. Dabei erhält der Angreifer wiederum die Protokollinfor-

mation der Schicht 3 (Sendestation, Empfangsstation, logische Kanalnummern etc.) im Klartext.

Diese Vorgehensweise kann so lange fortgesetzt werden, bis die Nutzinformation aus verschlüsselten Daten besteht. Diese Verschlüsselung befindet sich im Beispiel von Abb. 15.5 am unteren Rand der Schicht N. Die verschlüsselten Daten müssen vor dem weiteren Auspacken entschlüsselt werden. Ist dem Angreifer das Entschlüsseln nicht möglich, so bleibt ihm auch der Zugang zu weiteren Informationen höherer Schichten und den Anwendungsdaten verwehrt.

Das Erschließen der Signale muß nicht unbedingt über das Abhören („Anzapfen“) des Übertragungsmediums geschehen. Sende- bzw. Empfangsgeräte verursachen während der Bearbeitung der übertragenen Daten elektromagnetische Abstrahlung, welche zur Rekonstruktion dieser Daten z.T. über große Entfernungen (bei PCs mit mittlerer Abstrahlung bis zu 200 m, siehe [Nitz_95]) genutzt werden kann. Ebenso modulieren die Geräte Informationen auf das Spannungsnetz, an dem sie angeschlossen sind. Je nach Übertragungs- bzw. Verarbeitungstechnik können weitere ungewollte Modulationen auftreten, welche zum Ausspähen von Informationen – oder nichtinterpretierbarer Daten, die eventuell wiedereingespielt werden können – genutzt werden können. Ebenso bedürfen laut [Engb_93] Richtfunkstrecken der besonderen Sicherung zum Schutz gegen ausländische und inländische Organisationen.

Zusammenfassung

Die folgenden Aussagen fassen die zu beachtenden Aspekte zusammen:

1. Sicherheitsfunktionalität kann grundsätzlich nur innerhalb eines Vertrauensbereichs realisiert werden. Vertrauensbereiche können dabei Anwendungen, Endgeräte, sichere Module etc. sein, die die korrekte Implementierung gewährleisten und ein Ausspähen (d.h. Angriffe auf die Sicherheitsfunktionalität) bzw. einen Nachbau mit technischen Mitteln aussichtslos gestalten.
2. EzE-Sicherheitsfunktionalität ist nur oberhalb der EzE-Grenzlinie integrierbar.
3. LzL-Sicherheitsfunktionalität ist nur unterhalb der LzL-Grenzlinie integrierbar.
4. Daten bzw. Informationen sind innerhalb und außerhalb des erzeugenden Knotens nur dann geschützt, wenn sie oberhalb der Sicherheitsfunktionalität anfallen.
5. Die EzE-Grenzlinie verhindert dabei den Schutz von Vermittlungsdaten EzE. Dies kann allenfalls mit KzK- oder LzL-Funktionen realisiert werden, wobei dann Vertrauensbereiche innerhalb aller genutzten Netzknoten ge-

schaffen werden müssen, um die entsprechende Sicherheitsfunktionalität integrieren zu können.

15.4 Allokation von Sicherheitsfunktionen im OSI-Referenzmodell

Die in den vorangegangenen Abschnitten diskutierten Sicherheitsfunktionen werden nun auf ihre Plazierungsmöglichkeiten im OSI-Referenzmodell untersucht. Eine ansatzweise Einordnung von Sicherheitsfunktionen in die verschiedenen Schichten findet sich in [ISO1_89]. Die vorliegende Arbeit hat zum Ziel, die verschiedenen Allokationspunkte hinsichtlich ihrer Auswirkung auf die erreichbare Sicherheit zu prüfen und dabei auch das Zusammenspiel von Komponenten zu berücksichtigen.

Horizontale und vertikale Verfeinerung des Grundmodelles

Ein Kommunikationsnetz kann zur Untersuchung von Allokationsmöglichkeiten für Sicherheitsfunktionen in eine vertikale und in eine horizontale Sicht aufgeteilt werden. Die horizontale Verfeinerung beschreibt die Projektion möglicher Sicherheitsmechanismen innerhalb einer Schicht auf verschiedene Komponenten des Teilnehmer- bzw. Netzbereiches. Die vertikale Verfeinerung beschreibt die Allokation der Sicherheitsmechanismen innerhalb einer Komponente auf verschiedenen Schichten.

Horizontale Verfeinerung:

- Übertragungsabschnitte (Leitungen, Richtfunkstrecken, Funkzellen),
- erweiterte Netzknoten (Netzübergänge, Vertrauenswürdige Instanzen),
- Netzknoten (Vermittlungsknoten),
- Netzabschluß (Teilnehmeranschlußbuchse, Nebenstellenanlage - NT1/2 im ISDN) und
- Teilnehmerknoten (Teilnehmer-Endgeräte wie Rechner bzw. Telefon, Black-Box).

Vertikale Verfeinerung:

- Bedienung der Anwendung (Nutzung bzw. organisatorische / betriebliche Verfahren, etc.),
- Anwendung und
- OSI-Schichten 1-7.

Die beiden folgenden Unterabschnitte untersuchen diese beiden Sichten zunächst getrennt. Anschließend wird am Beispiel des Diensteintegrierenden Digitalnetzes (ISDN) untersucht, wo Sicherheitsfunktionen integriert werden können und wie sie zusammenwirken.

Verfeinerung in der Vertikalen

Die Funktionalität eines Kommunikationsnetzes wie auch jedes Knotens läßt sich entsprechend ihrer Aufgaben in sogenannten Schichten gruppieren [ISO2_89]. Jede dieser Schichten entspricht einer bestimmten Abstraktion des Kommunikationsvorganges. Im folgenden werden alle Schichten sowie die Anwendungsebene und die Bedienungsebene aus Sicherheitssicht beschrieben und mögliche Schutzmaßnahmen vorgestellt. Eine zentrale Aufgabe ist die Einordnung der passenden Sicherheitsfunktionalität an der richtigen Stelle. Dies unterstützt die effiziente Erfüllung der Sicherheitsanforderungen.

Die folgende Tabelle zeigt zusammenfassend die Allokationsmöglichkeiten für Sicherheitsmechanismen. Ein „x“ kennzeichnet Möglichkeiten für die Plazierung von Funktionalität.

Schicht / Knoten	Ü-Abschnitt	erweiterter Netzknoten	Netz-knoten	Netzab-schluß	Teilneh-merknoten
Bedienung der Anwendung					X
Anwendung		X			X
Schichten 4 - 7		X			X
Schichten 1 - 3		X	X	X	X

Tabelle 15.1: Funktionsgruppen im Kommunikationsnetz und im Teilnehmeranschlußbereich

Auf Allokationsmöglichkeiten innerhalb der *Schichten 1-7* wird in Abschnitt 15.5 am Beispiel des ISDN näher eingegangen.

Die *Anwendung* bietet den optimalen Ausgangspunkt für den Schutz von Daten, die durch sie verarbeitet werden. Daten können vor dem Abspeichern auf einem Speichermedium bzw. dem Versenden über Netze geschützt werden. Dadurch entfallen sämtliche Angriffspunkte unterhalb der Anwendung bezüglich der Anwendungsdaten. Nicht geschützt werden dadurch alle anfallenden Protokolldaten und die Verfügbarkeit der Daten.

Im Bereich der *Bedienung und Anwendung* muß vor allem der Zugang und Zugriff auf das System gesichert werden. Auf dieser Ebene sind viele bekannte Angriffe durch erratene bzw. gestohlene Paßwörter einzuordnen. Sicherheitsme-

chanismen sind hier in Form organisatorischer Verfahren möglich. Das Einhalten von durchdachten (Sicherheits-) Richtlinien und Aspekte der Ergonomie der Schnittstellen der Sicherheitsmechanismen zum Anwender (Paßwortwahl, korrektes Bedienen einer Anwendung) spielen bei der Sicherung von Informationen eine entscheidende Rolle. Beispielsweise können viele Textverarbeitungssysteme Texte unter verschiedenen Zugriffsberechtigungen abspeichern. Dabei kann durch geeignete Voreinstellungen dafür gesorgt werden, daß die Standardeinstellung für die Abspeicherung von Texten nur Rechte für den Autor vorsieht.

Verfeinerung in der Horizontalen

Die im vorigen Unterabschnitt motivierten potentiellen Sicherheitsmechanismen können zur Realisierung der verschiedenen Anforderungen (Vertraulichkeit, Integrität und Verfügbarkeit) auf verschiedene Komponenten verteilt werden.

Netzinterne Komponenten können Vertrauensbereiche in Form von Sicheren Modulen beinhalten [PfPf_95], die Sicherheitsfunktionalität beherbergen können und im Zusammenspiel ebenfalls Sicherheitsfunktionalität zwischen Sender und Empfänger erbringen können.

Die folgenden Abschnitte befassen sich vor allem mit der Frage, wie die verschiedenen Sicherheitsfunktionen verschiedener Schichten auf vorhandene Komponenten (Endgerät, Netzabschluß, Netzknoten) bzw. additiv hinzufügbare Komponenten (Black-Box, erweiterter Netzknoten) verteilt werden können.

Sicherheitsfunktionalität innerhalb des Teilnehmerbereiches: Netzabschluß, Endgerät und Black-Box bieten sich als Träger für Sicherheitsfunktionalität zum Schutz von Teilnehmerdaten besonders an.

Eine Black-Box bezeichnet hier eine separate Komponente innerhalb des Teilnehmerbereiches. Der Aufwand für diese zusätzliche Komponente ist allerdings relativ hoch, da alle Schichten unterhalb der beabsichtigten Sicherheitsschicht zusätzlich implementiert werden müssen, um eine logische Zwischenschicht einfügen zu können. Solche Black-Box-Geräte werden zunehmend im LAN-Bereich angeboten [Pohl_95], um Rechner mit erhöhten Sicherheitsanforderungen ohne Änderungen der Software (Anwendungen, Betriebssysteme, Kommunikationssoftware etc.) gegen Angriffe aus dem Kommunikationsnetz zu sichern.

Diese Komponenten können vom Teilnehmer selbst installiert, kontrolliert und überwacht werden. Gegebenenfalls kann sogar aus einer Menge von unabhängigen Anbietern ausgewählt werden. Dies alles erhöht das Vertrauen der Teilnehmer in diese Komponenten und damit auch das Vertrauen in die Sicherheit der darin realisierten Funktionalität. Die Verteilung von Sicherheitsfunktionali-

tät auf mehrere Komponenten und Hersteller verhindert bzw. vergrößert den Aufwand für einzelne Angreifer, die verteilte Sicherheitsfunktionalität im Gesamten anzugreifen.

Beispielsweise könnte eine *kanonische Verteilung* die Sicherheitsmechanismen immer möglichst an den Rand des Vertrauensbereiches legen. Dieser Ansatz unterstützt beispielsweise das mehrfache Verwenden der Sicherheitsfunktionalität im Netzabschluß und damit auch die Wirtschaftlichkeit der Sicherheitsfunktionen. Der Nachteil besteht darin, daß die Funktionalität universell sein muß und deshalb nicht auf spezielle Endgeräte bzw. Anwendungen zugeschnitten werden kann.

Abb. 15.6 zeigt die kanonische Verteilung von Sicherheitsfunktionen am Beispiel zweier Teilnehmerbereiche, die über ein Endgerät, eine Black-Box (zusätzliche, maßgeschneiderte Sicherheitsfunktionalität) und einen Netzabschluß verfügen. Der Vertrauensbereich erstreckt sich in diesem Beispiel mindestens über die Komponenten des Teilnehmerbereiches.

Die gestrichelten Allokationsbereiche für LzL-Sicherheitsfunktionen zwischen Komponenten innerhalb des Teilnehmerbereiches deuten an, daß sie lediglich Bedeutung erlangen, falls zwar die Komponenten, nicht aber deren Verbindungsleitungen innerhalb des Vertrauensbereiches liegen.

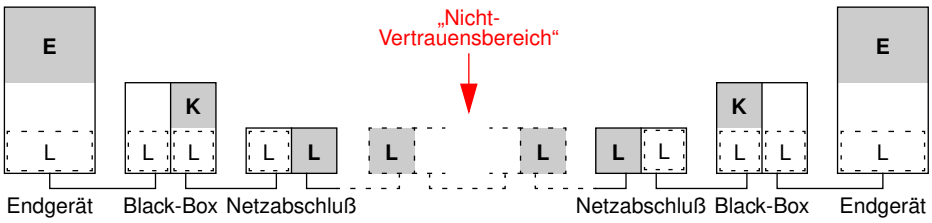


Abbildung 15.6: Vertikale Verteilung von Sicherheitsfunktionen im Teilnehmerbereich

Sicherheitsfunktionen in den *Netzabschluß* zu verlagern, bietet Endgeräte- und Anwendungs-Unabhängigkeit. Der Aufwand der nachträglichen Integration von Sicherheitsfunktionen kann sich dadurch auf verschiedene Endgeräte (im Falle eines PBX) und verschiedene Anwendungen (Fax, Telefondienst, Datenübertragung) verteilen. Moderne Kommunikationsanlagen bieten bereits Sicherheitsfunktionen auf der Anwendungsebene an [Blab_95].

Duale EzE-Sicherheitsfunktionen – in Endgerät oder Black-Box – sind notwendig, falls LzL-Sicherheitsfunktionen aufgrund fehlender Vertrauensbereiche in

den Knoten des Kommunikationsnetzes nicht einsetzbar sind oder um sogenannte Gaps auszugleichen (siehe Abb. 15.2).

Anwendungsnahe bzw. endgerätespezifische Sicherheitsfunktionen müssen im *Endgerät* selbst realisiert werden (z.B. bei mobilen Endgeräten).

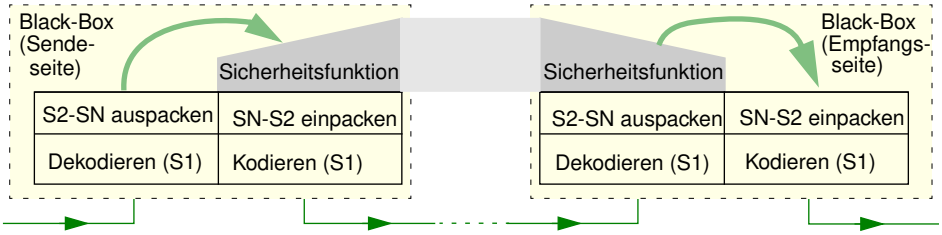


Abbildung 15.7: Aufbau einer Black-Box auf Sende- und Empfangsseite

In einer Black-Box werden die eingehenden Daten bis zur Schicht N (SN) ausgepackt (Abb. 15.7). Oberhalb dieser Schicht werden sie gesichert und standardkonform wieder verpackt, kodiert und auf den abgehenden Übertragungsabschnitt weitergeleitet. Die entsprechende duale Sicherheitsfunktionalität muß auf der Empfängerseite implementiert werden.

Nach Abb. 15.7 realisierte Sicherheitsfunktionen können aufgrund der aufwendigen Operationen zum Aus- und Einpacken von Datenpaketen für N > 1 meist keine Zeittransparenz bieten und sind deshalb für Echtzeitanwendungen mit geringer maximaler Verzögerungszeit nicht anwendbar. Sehr gut einsetzbar ist eine Black-Box z.B. zur nachträglichen Sicherung von Punkt-zu-Punkt-Verbindungen. Eine solche Black-Box braucht lediglich die digitalen Signale dekodieren, verschlüsseln und kodiert weiterleiten (N=1).

Verteilung von Sicherheitsfunktionen innerhalb des Netzes: Netzkomponenten sind nicht vom Teilnehmer auswählbar, kontrollierbar oder überwachbar. Deshalb befinden sie sich aus Sicht des Teilnehmers zunächst grundsätzlich außerhalb des Vertrauensbereiches der Teilnehmer. Protokolldaten der Schichten 2 und 3 können in Vermittlungsnetzen i.a. nicht EzE geschützt werden, da sie für die zwischenliegenden Netzknoten nicht transparent sind. Zu ihrem Schutz bieten sich dem Teilnehmer prinzipiell zwei Möglichkeiten:

- **Vermeidung schützenswerter Protokolldaten:** Dies ist in bestehenden Netzen wegen der Adressierung nur durch die Schaffung von Anonymitätsgruppen bei gemeinsam genutzten Netzadressen oder durch Broadcast-Funktionen zur Vermeidung von Adressierinformation erreichbar.

Gemeinsam genutzte Netzadressen realisieren eine Anonymitätsgruppe, wobei einzelne Rufe nicht über eine Netzadresse eindeutig einem Teilnehmer zuordenbar sind. Ein Spezialfall gemeinsam genutzter Netzadressen sind die Funkzellen in Mobilfunknetzen.

In Broadcast-Medien (LANs, Funknetzen etc.) kann durch implizite Adressierung [Pfit_90, S.64] die Station eine an sie gerichtete Nachricht erkennen, ohne daß außerhalb der Station beobachtbar ist, für welchen Teilnehmer die Nachricht bestimmt war, es sei denn die empfangende Station verrät sich durch eine zeitlich mit der empfangenen Nachricht korrelierte Reaktion z.B. durch sofortige Bestätigung der Nachricht.

- **Schaffung von Vertrauensbereichen innerhalb des Kommunikationsnetzes:** Vertrauensbereiche sind Voraussetzung für die Integration von Sicherheitsfunktionen zur Sicherung von Protokolldaten innerhalb des Kommunikationsnetzes, z.B. durch die Realisierung temporärer Identitäten (siehe z.B. [KeFe_96]). Solche Vertrauensbereiche können von unabhängigen Instanzen zertifizierte, überwachte und gewartete sichere Module oder spezielle erweiterte Netzknoten sein, die vertrauenswürdige Funktionen bereitstellen.

Es gibt allerdings auch Ausnahmen von der o.a. Behauptung, daß die Protokolldaten der Schicht 3 nicht EzE geschützt werden können. Lt. [ATMF_97] werden für ATM-Netze (Asynchronous Transfer Mode) spezielle Informationselemente diskutiert, die einzelne Nachrichtenbestandteile (beispielsweise Adressen) während ihrer Übertragung zwischen den Teilnehmervermittlungsstellen vor unerkannter Veränderung schützen. Dazu wird über schützenswerte Nachrichtenteile ein Hash-Wert berechnet und dieser verschlüsselt in jenem speziellen Informationselement transparent für Zwischenknoten übertragen. Der Empfänger kann die Integrität der geschützten Nachrichtenteile anhand des speziellen Informationselementes prüfen.

15.5 Allokation von Sicherheitsfunktionen im ISDN

In diesem Abschnitt wird die Allokation von Sicherheitsfunktionen am Beispiel des Diensteintegrierenden Digitalnetzes (Integrated Services Digital Network, [Sieg_92,Mant_91,Q9xx_89]) besprochen. Abb. 15.8 zeigt eine verbreitete Konfiguration im ISDN. Am ISDN-Basisanschluß können mehrere Endgeräte über einen Bus (S-Schnittstelle) gleichzeitig betrieben werden. Das ISDN arbeitet verbindungsorientiert, d.h. bevor Daten zwischen Endgeräten ausgetauscht werden können, muß eine entsprechende Verbindung hergestellt werden.

Die Funktionalität des ISDN verteilt sich auf ISDN-Endgeräte, den Netzabschluß (NT) und die ISDN-Vermittlungsstellen. Der NT schließt den Verantwor-

tungsbereich der Netzbetreiber bzw. Dienstanbieter gegen den Verantwortungsbereich der Teilnehmer ab.

Auf der Protokollebene (kommunikations- und anwendungsunterstützende Protokolle) werden Funktionen zur Unterstützung der Übermittlung von Steuerdaten und Nutzdaten unterschieden.

Zur Übertragung von Steuernachrichten stehen allen Endgeräten an einem Teilnehmeranschluß gemeinsam 16 kbit/s zur Verfügung. Zur Übertragung von Nutzdaten stehen am ISDN-Basisanschluß zwei Nutzdatenkanäle, die sogenannten B-Kanäle, mit einer Nutzdatenrate von je 64 kbit/s zur Verfügung.

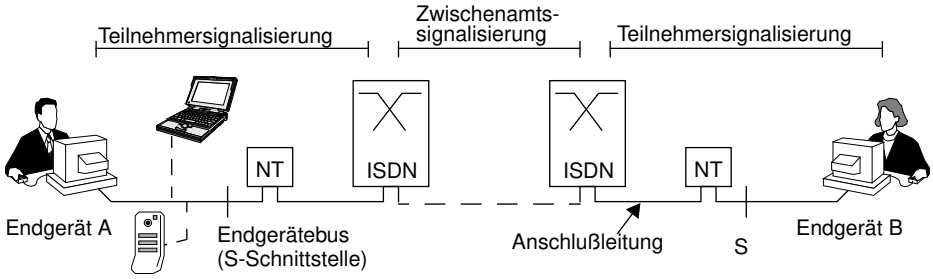


Abbildung 15.8: Konfiguration am ISDN-Basisanschluß

Steuerung von Diensten im ISDN: Die Funktionen zur Übermittlung von Steuernachrichten zwischen verschiedenen Knoten werden i.a. als Signalisierung bezeichnet. Im ISDN wird unterschieden zwischen

- *Teilnehmersignalisierung* zur Übermittlung von Steuernachrichten zwischen Endgeräten und ISDN-Teilnehmervermittlungsstellen (TVSt) und
- *Zwischenamtssignalisierung* zur Übermittlung von Steuernachrichten zwischen ISDN-Vermittlungsstellen.

Die Funktionen zur Unterstützung des Austauschs von Steuernachrichten an der Teilnehmer-Netz-Schnittstelle im ISDN werden als D-Kanal bezeichnet. Die *Verbindungssteuerung* baut auf dieser *Teilnehmersignalisierung* auf und steuert durch Austausch von Steuerinformation z.B. den Aufbau und Abbau von Verbindungen. Sie nutzt dazu die Funktionen des ISDN-D-Kanals (D-1, D-2, D-3 in Abb. 15.9) zur Übermittlung von Steuerinformation zwischen Steuerprozessen im Endgerät und in der Teilnehmervermittlungsstelle. Die Protokolle des D-Kanals regeln u.a. die Adressierung und den Aufbau logischer Verbindungen (D-3) zwischen Endgerät und TVSt, die Erkennung und Behandlung von Übertragungsfehlern und eine Reihenfolgesicherung (D-2) sowie die Kodierung der

Informationen und den Zugang zum Übertragungsmedium (D-1). Die *Verbindungssteuerungsprozesse* in den Endgeräten und den Netzknoten des Verbindungsweges sorgen im Zusammenspiel für die Durchschaltung eines transparenten Nutzdatenkanals (B-Kanal), der anschließend den Anwendungen in den Endgeräten zur transparenten Übertragung von Nutzdaten zur Verfügung steht.

Die Steuernachrichten des Teilnehmerbereiches werden in den Teilnehmervermittlungsstellen verarbeitet und in *Steuernachrichten des Zwischenamtsbereiches* umgesetzt. Die Definition der im Zwischenamtsbereich ausgetauschten Steuernachrichten ist durch den ISDN-UserPart (ISUP) vorgegeben. Der ISUP definiert auch anwendungsunterstützende Funktionen der Netzknoten zum Austausch von Steuernachrichten (*Zwischenamtssignalisierung*); auf Protokolle darunterliegender Schichten zur gesicherten Übertragung von Steuernachrichten zwischen Vermittlungsstelle kann hier nicht näher eingegangen werden.

Die Prinzipien der Signalisierung im Zwischenamtsbereich (Common Channel Signalling, CCS) sollen hier nicht weiter betrachtet werden. Für die Untersuchung von Allokationsmöglichkeiten ist aber bedeutsam, daß es Informationselemente (Paramter von Steuernachrichten) gibt, welche von der Zwischenamtssignalisierung transparent übertragen werden. Solche Informationselemente können innerhalb eines Endgerätes in gewöhnliche Signalisiernachrichten der Schicht 3 (D-3) eingebettet werden. An der Netzgrenze werden sie in Nachrichten der Zwischenamtssignalisierung eingebettet und transparent übertragen; die gegenüberliegende Teilnehmervermittlungsstelle setzt diese sog. User-User-Informationen in Signalisiernachrichten der Teilnehmersignalisierung ein und zeigt sie somit dem empfangenden Endgerät an. Diese User-User-Informationselemente eignen sich daher auch als Transportmedium für gesicherte Informationsträger, welche zwischen Sicherheitsfunktionen in verschiedenen Endgeräten ausgetauscht werden sollen.

Nutzdaten im ISDN: Zur Bearbeitung von Nutzdaten steht im ISDN lediglich Funktionalität zur Kodierung und zum Zugriff auf das Übertragungsmedium zur Verfügung. Diese Funktionen werden der Schicht 1 zugeordnet (B-1). Fehlersicherungen und weitere unterstützende Funktionen müssen gegebenenfalls durch die Anwendung realisiert werden. Die *Anwendung* wird dabei durch Funktionen der Endgeräte zur Erzeugung und Verarbeitung von Nutzdaten definiert.

Funktionen sind im ISDN also charakterisiert durch:

- den Knoten, in dem sie realisiert sind,
- die Art der durch sie verarbeiteten Daten (Steuerdaten, Nutzdaten, Managementdaten) und

- der Schicht des OSI-Referenzmodelles, der ihre Funktionalität zuordenbar ist.

Zur Unterscheidung werden Funktionen zur Verarbeitung von Steuerdaten mit „D“, Funktionen zur Verarbeitung von Nutzdaten mit „B“ bezeichnet.

Allokationsmöglichkeiten für Sicherheitsfunktionen im ISDN: Der Auf- und Abbau von Verbindungen sowie die Steuerung zusätzlicher Dienstmerkmale erfolgt durch die Verbindungssteuerung. Diese erzeugt Signalisiernachrichten, welche anschließend die Funktionen des Signalisierprotokollturms (D-3, D-2, D-1) im Endgerät durchlaufen bevor sie über das Übertragungsmedium an die Vermittlungsstelle gesendet werden (siehe auch Abb. 15.9). Zum Aufbau einer Verbindung und zur Koordination der Steuerung der beteiligten Teilnehmeranschlüsse werden auch Signalisiernachrichten zwischen den entsprechenden Teilnehmervermittlungsstellen – genauer zwischen den entsprechenden Verbindungssteuerungen – ausgetauscht.

Für die Behandlung von Nutzdaten ist im ISDN lediglich Funktionalität für die Kodierung von Anwendungsdaten für ihren Transport zur Vermittlungsstelle (B-1 in Abb. 15.10) vorgesehen. Innerhalb des ISDN werden die digital übertragenen Daten in den ISDN-Vermittlungsstellen lediglich in verschiedene Puffer umkopiert und so zwischen verschiedenen Leitungen und Zeitlagen vermittelt.

Schicht \ Knoten	TE	NT	ISDN-VSt	Black-Box
Anwendung	B,D	–	D	B,D
Schicht 3	(B),D	–	D	B,D
Schicht 2	(B),D	–	D	B,D
Schicht 1	B,D	B,D	B,D	B,D

Tabelle 15.2: Funktionsverteilung am ISDN-Basisanschluß aus Teilnehmersicht

Für die folgenden Untersuchungen sind vor allem die für Sicherheitsfunktionen relevanten Knoten und die darin implementierten bzw. implementierbaren Schichten interessant. Die folgende Tabelle faßt die prinzipiellen Allokationsmöglichkeiten für Sicherheitsfunktionen am ISDN-Basisanschluß zusammen. Die eingeklammerten Nutzkanalfunktionen können (z.B. im Falle von Paketdiensten), müssen aber nicht (z.B. beim Fernsprechdienst) implementiert sein.

Tabelle 15.2 zeigt, daß zur Sicherung von Nutzdaten (B-Kanal) die Anwendung innerhalb des Endgerätes oder eine nach Abb. 15.7 aufgebaute Black-Box mit Sicherheitsfunktionalität angereichert werden können. Weiterhin kann Sicherheitsfunktionalität innerhalb oder an der oberen Grenze von Schicht 1 in das

Endgerät, den Netzabschluß (NT) oder die Vermittlungsstelle (ISDN-VSt) integriert werden.

Für die Sicherung von Signalisierdaten (D) kann Funktionalität auch in höhere Schichten der ISDN-Vermittlungsstelle integriert werden. Der NT beinhaltet Funktionen zur Umkodierung von Signalen (D-1, B-1). Weitere Funktionen zur Aktivierung des ISDN-Anschlusses etc. sollen hier nicht betrachtet werden und haben auf die Allokation möglicher Sicherheitsfunktionen keine Auswirkungen – wohl aber auf deren Implementierung, z.B. in Bezug auf ihre Synchronisierung.

Innerhalb des NT stehen also nur die Funktionen der Schicht 1 zur Anreicherung mit Sicherheitsfunktionen zur Verfügung.

Allokation von Sicherheitsfunktionen: Tabelle 15.3 klassifiziert Sicherheitsfunktionen, welche innerhalb der jeweiligen Komponenten plaziert werden können. Es werden ausschließlich Plazierungsalternativen betrachtet, bei welchen duale Sicherheitsfunktionen verschiedener Teilnehmerbereiche in äquivalenten Komponenten realisiert sind. In Klammern angegebene Allokationsmöglichkeiten sind nicht symmetrisch (z.B. Verschlüsselungsfunktion in TE-A und Entschlüsselungsfunktion in NT-B). Doppelt geklammerte Allokationsmöglichkeiten sind eher theoretischer Natur und bieten sich für eine praktische Implementierung aus mehreren Gründen nicht an.

Sicherung zwischen	TE-A	NT-A	ISDN-VSt A	TE-B	NT-B	ISDN-VSt B
TE-A	–	LzL	KzK	EzE	(KzK)	((KzK))
NT-A	LzL	–	LzL	(KzK)	KzK	((KzK))
ISDN-VSt A	KzK	LzL	–	((KzK))	((KzK))	KzK
TE-B	EzE	(KzK)	((KzK))	–	LzL	KzK
NT-B	(KzK)	KzK	((KzK))	LzL	–	LzL
ISDN-VSt B	((KzK))	((KzK))	KzK	KzK	LzL	–

Tabelle 15.3: Klassifikation möglicher Sicherheitsmechanismen am ISDN-Basisanschluß

Die Kommunikationsrichtung wird in der Tabelle nicht unterschieden. Die symmetrische Anordnung dualer Sicherheitsfunktionen erleichtert die Realisierung von – für das zwischenliegende Netz – transparenten Sicherheitsfunktionen und damit deren Integrationsfähigkeit. Eine Ausnahme bildet die Black-Box, welche zur Aufnahme von Sicherheitsfunktionen prinzipiell an jeder Stelle am

Teilnehmeranschluß – mit unterschiedlichem Aufwand – eingefügt werden kann.

Die Integration von Sicherheitsfunktionen in eine der dargestellten Komponenten kann i.a. durch direkte Implementierung der Funktion innerhalb der Komponente oder entsprechend Abb. 15.7 durch Vor- bzw. Nachschalten einer Black-Box realisiert werden.

Stellvertretend für viele denkbare Sicherheitsanforderungen sollen die folgenden durch Integration von Sicherheitsmechanismen in die Konfiguration aus Abb. 15.8 garantiert werden:

1. sichere Identifikation von Teilnehmer und Dienstanbieter bzw. Netzbetreiber,
2. Integrität und Vertraulichkeit der Signalisiernachrichten, welche zwischen Teilnehmer und Vermittlungsstelle ausgetauscht werden,
3. sichere Identifikation der Kommunikationspartner A und B und
4. Integrität und Vertraulichkeit der Nutzdaten, welche zwischen A und B ausgetauscht werden.

Abb. 15.9 und Abb. 15.10 zeigen die funktionale Sicht auf den ISDN-Basisanschluß. Abb. 15.9 zeigt Funktionen zur Steuerung des Netzes, während Abb. 15.10 die Funktionen zur Behandlung der Nutzdaten darstellt.

Grenzlinien für die Allokation von Sicherheitsfunktionen: Die Bezugspunkte für die Betrachtung von EzE-, KzK- und LzL-Grenzlinien folgen aus den oben genannten Sicherheitsanforderungen. Die zu sichernde übergeordnete Beziehung besteht hier zwischen den Endgeräten. Deshalb dienen diese als Bezugspunkte für die Klassifikation der Sicherheitsfunktionen. Als Bezugspunkte sind folglich gegeben:

- Endgerät A und Vermittlungsstelle A bzw. Endgerät B und Vermittlungsstelle B bezüglich KzK-Funktionen (Anforderungen 1. und 2.)
- Endgerät A und Endgerät B bezüglich EzE-Funktionen (Anforderungen 3. und 4.)
- LzL-Funktionen werden nicht vorgesehen. Da der NT zwischen Endgerät und Vermittlungsstelle liegt, besteht keine direkte Sicherungsbeziehung zwischen benachbarten Knoten. Die Realisierung übergeordneter Sicherheitsfunktionen durch die Aneinanderreihung von LzL-Funktionen unter Einbeziehung des NT (z.B. Endgerät - NT und NT - Vermittlungsstelle) wird an dieser Stelle als zu aufwendig betrachtet.

Mit diesen Bezugspunkten sind gleichzeitig die vertikalen Allokationspunkte für Sicherheitsfunktionen festgelegt.

EzE-Grenzlinien für Funktionen zwischen den Endgeräten A und B:

- Die *EzE-Grenzlinie für Nutzdaten* liegt in Abb. 15.10 am oberen Rand von Schicht 1 (B-1), da die zwischen den Endgeräten liegenden Knoten (NT, Vermittlungsstellen) die Nutzdaten umkodieren (Schicht 1-Funktion).
- Die *EzE-Grenzlinie für Steuerdaten* liegt in Abb. 15.9 für die oben genannten User-User-Informationselemente am oberen Rand von Schicht 3 (D-3), da diese Informationselemente transparent zwischen Endgeräten ausgetauscht werden können. Alle anderen Steuerdaten werden beim Übergang zur Zwischenamtssignalisierung im ISDN verarbeitet und sind deshalb nicht transparent.

KzK-Grenzlinien für Funktionen zwischen Endgerät und Vermittlungsstelle bzw. Dienst:

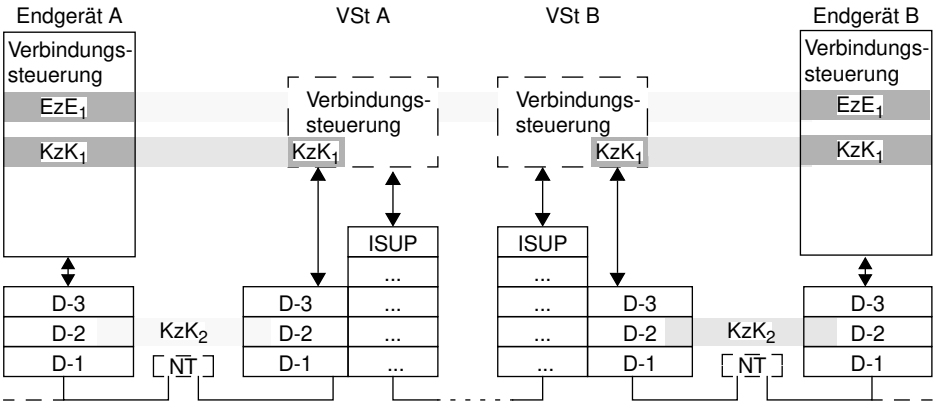
- Die *KzK-Grenzlinie für Nutzdaten* (Abb. 15.10) liegt theoretisch oberhalb von Schicht 1 (B-1), da der zwischen Endgerät und Vermittlungsstelle liegende Knoten (NT) Funktionen dieser Schicht umsetzt. In der Vermittlungsstelle verbleiben keine Schichten zur Anreicherung mit KzK-Funktionen oberhalb der Grenzlinie. Zur Integration von KzK-Funktionen müßte die Vermittlungsstelle entsprechend oberhalb von Schicht 1 mit – für den NT transparenter – Funktionalität angereichert werden. KzK-Funktionen für Nutzdaten werden zur Garantie der oben genannten Anforderungen nicht hinzugezogen.
- Die *KzK-Grenzlinie für Steuerdaten* (Abb. 15.9) liegt oberhalb von Schicht 1 (D-1), da der NT auch die Steuerdaten der Schicht 1 umkodiert.

LzL-Grenzlinien für Funktionen in benachbarten Knoten (Endgerät-NT, NT-VSt, VSt-VSt):

- Die *LzL-Grenzlinie für Nutzdaten und Steuerdaten* zwischen Endgerät und Vermittlungsstelle liegt am oberen Rand von Schicht 1 (B-1, D-1). Innerhalb des Netzes liegt die LzL-Grenzlinie für Nutzdaten auf Schicht 1 und für Signalisierdaten auf Schicht 3. Der NT bestimmt also die Lage der LzL-Grenzlinie im Teilnehmerbereich. Es ist jedoch denkbar, daß die im Teilnehmerbereich durch KzK-Funktionen realisierte Sicherung (Überbrückung des NT) innerhalb des Netzes durch LzL-Funktionen fortgesetzt wird. Ein Beispiel für eine solche Funktion stellt die Fehlersicherung nach dem HDLC-Protokoll dar, welche im Teilnehmerbereich als KzK-Funktion, innerhalb des Netzes jedoch als LzL-Funktion realisiert ist.

Festlegung der horizontalen Allokationspunkte: Zur sicheren Bestimmung der Identität von Teilnehmer und Dienstanbieter bzw. Netzbetreiber werden Funktionen zur Authentikation in die Verbindungsbehandlung von Endgerät und Vermittlungsstelle integriert (Funktionalität KzK_1 in Abb. 15.9).

Während der Prüfung der Identität wird innerhalb der Authentikation ein gemeinsamer geheimer Sitzungsschlüssel (K_{KzK}) zwischen Endgerät und Vermittlungsstelle vereinbart (Anforderung 1.).



EzE_1: Authentikation und Schlüsselaustausch (K_{EzE}) zwischen Endgerät A und Endgerät B
KzK_1: Authentikation und Schlüsselaustausch (K_{KzK}) zwischen Teilnehmer und TVSt
KzK_2: Kryptographische Sicherung von Steuerdaten mit K_{KzK} zwischen Endgerät und TVSt

Abbildung 15.9: Steuerung und Signalisierprotokolle im ISDN

Zur Sicherung der Steuernachrichten zwischen Endgerät und Vermittlungsstelle werden kryptographische Funktionen in Schicht 2 (D-2) der Signalisierung in Endgerät und Vermittlungsstelle integriert (KzK_2 in Abb. 15.9), welche mit dem gemeinsamen Sitzungsschlüssel K_{KzK} parametrisiert werden (Anforderung 2.).

Die Identitätsprüfung zwischen den Teilnehmern wird durch Integration von Authentikationsfunktionalität in die Endgeräte realisiert (EzE_1 in Abb. 15.9). Die Funktionalität wird in die Verbindungssteuerung integriert und nutzt die oben beschriebenen User-User-Informationselemente zum Austausch der Authentikationsnachrichten zwischen den Endgeräten und zur Installation eines gemeinsamen geheimen Sitzungsschlüssels K_{EzE} (Anforderung 3.).

Zum Schutz der Nutzdaten zwischen A und B werden Sicherheitsfunktionen transparent für die Anwendung oberhalb der Schicht 1 (B-1) in den Endgeräten integriert (EzE_2 in Abb. 15.10). Diese Sicherheitsfunktionen nutzen den gemeinsamen Schlüssel K_{EzE} zur Parametrisierung von kryptographischen Funktionen wie z.B. der Verschlüsselung (Anforderung 4.).

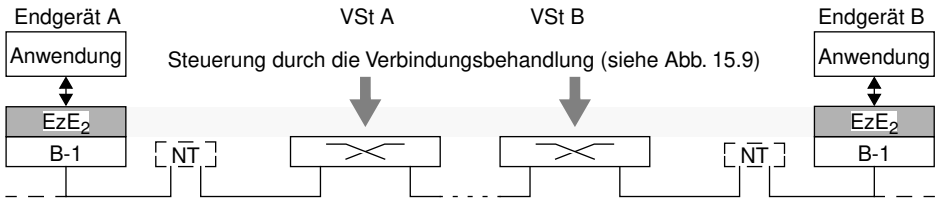


Abbildung 15.10: Nutzdatenprotokolle im ISDN

Ein Beispiel für die Realisierung der oben angesprochenen EzE-Funktionen zur Authentikation zwischen Teilnehmern im ISDN unter Zuhilfenahme von User-User-Informationselementen ist in [Sail_96] dargestellt. Die EzE-Sicherung der Nutzdaten zwischen den Teilnehmern erfolgt ähnlich wie die KzK-Sicherung der Steuerdaten zwischen Teilnehmer und Vermittlungsstelle. Die folgenden Abschnitte gehen etwas näher auf die Integration der angesprochenen KzK-Funktionen ein, die zwischen Endgerät und Vermittlungsstelle wirken.

Authentikation und Schlüsselaustausch zwischen Endgerät und VSt:
Die Authentikation und die Installation eines gemeinsamen Schlüssels zwischen Endgerät (Teilnehmer) und Vermittlungsstelle (Dienstanbieter, Netzbetreiber) erfolgen innerhalb der Verbindungsbehandlung im Endgerät und in der Teilnehmervermittlungsstelle. Diese Funktionalität kann in Form von Dienstmerkmalen implementiert werden. Es handelt sich hierbei um KzK-Funktionalität.

Während der Authentikation wird die Identität von Teilnehmer und Dienst auf der Basis eines Signatursystems [RiSh_78] geprüft. Voraussetzung dafür ist, daß jeder Identität (Teilnehmer, Dienstanbieter, Netzbetreiber, etc.) eindeutig ein geheimer Schlüssel zum Signieren und ein öffentlicher Schlüssel zur Prüfung der Signatur zugeordnet ist. Auf der geprüften Identität eines Teilnehmers können beispielsweise Zugriffskontrollmechanismen (Berechtigungsprüfung) und die Zuordnung von Gebühren aufbauen. Diese Mechanismen können vom physikalischen Anschluß entkoppelt werden und bilden damit die Grundlage für Teilnehmermobilität im Festnetz.

Zusätzlich wird während der Authentikation ein *gemeinsamer geheimer Sitzungsschlüssel* im Endgerät und in der Vermittlungsstelle installiert. Dieser ermöglicht die kryptographische Sicherung der Daten auf der Übertragungsstrecke zwischen Endgerät und Vermittlungsstelle. Dieser Schutz erscheint sinnvoll, wenn aufgrund neuer Anwendungen (Telebanking etc.) die Sicherheitsanforderungen an die kommunizierten Daten (Steuer- und Nutzdaten) steigen.

Die Verbindungssteuerung (Signalisierung) wird um Funktionen für die Authentikation und den Schlüsselaustausch angereichert (Auth). Die dabei zwischen Teilnehmer und Vermittlungsstelle auszutauschenden Authentikations-Nachrichten werden in standardisierte Schicht 3-Protokolldateneinheiten (PDU) integriert und zusammen mit den herkömmlichen Verbindungsaufbau-Nachrichten transparent für darunterliegende Schichten und den NT zwischen Teilnehmer und Vermittlungsstelle übertragen. Abb. 15.11 zeigt eine Realisierung und die Zuordnung der jeweiligen Funktionen der beteiligten Knoten Endgerät, NT und Vermittlungsstelle.

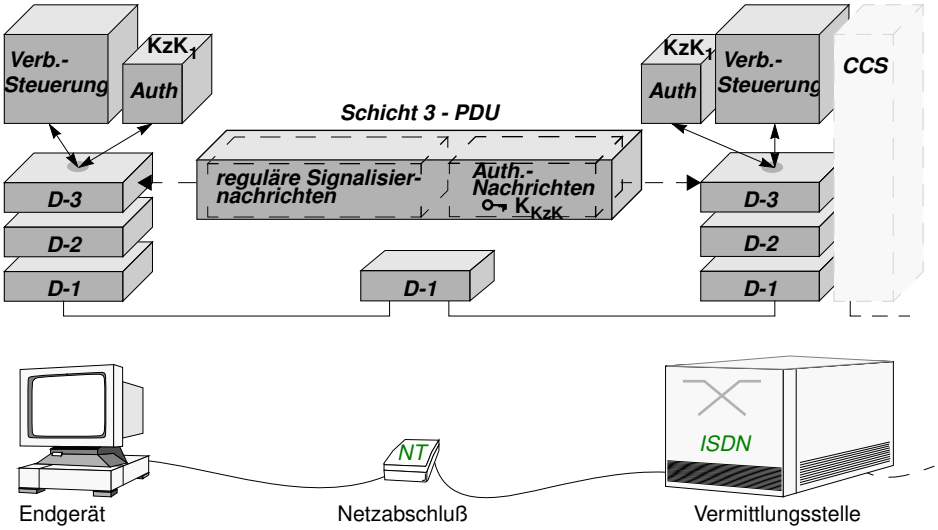


Abbildung 15.11: Authentikation und Schlüsselaustausch zwischen Endgerät und Vermittlungsstelle innerhalb der Teilnehmersignalisierung im ISDN – KzK-Funktionalität

Wird die Authentikation nach dem Vorbild der Dienstmerkmale im ISDN realisiert [BaGo_95], so können die Authentikationsnachrichten in sogenannten Facility-Informationselementen transparent für Schicht 3 übertragen werden. Da diese Funktionen transparent für den zwischenliegenden Netzabschluß (NT) realisiert werden, handelt es sich um KzK-Funktionalität.

Sicherung der Signalisierung zwischen Endgerät und Vermittlungsstelle:
Die Sicherung der Signalisiernachrichten zwischen Endgerät und Vermittlungsstelle (KzK_2) kann an der unteren Grenze von Schicht 2 integriert werden. Durch die oberhalb der Verschlüsselung gegebenen Fehlersicherungsfunktionen (Prüfsumme und Reihenfolgesicherung) ist sowohl die Integrität, als auch

die Vertraulichkeit der Signalisierdaten ohne das Hinzufügen weiterer Redundanz möglich.

Die von Schicht 3 an Schicht 2 zur gesicherten Übertragung übergebene Dateneinheit (Service Data Unit, SDU) wird – gesteuert durch die ebenfalls übergebene Kontrollinformation (Interface Control Information, ICI) – zunächst mit einem Header versehen, der u.a. eine fortlaufende Nummer zur Reihenfolgesicherung des übertragenen Schicht 2-Rahmens enthält. Zusätzlich wird eine Prüfsumme berechnet, um zufällige Übertragungsfehler sicher zu erkennen. Diese Prüfsumme wird über den Header und die Schicht 3 - SDU berechnet (siehe Abb. 15.12).

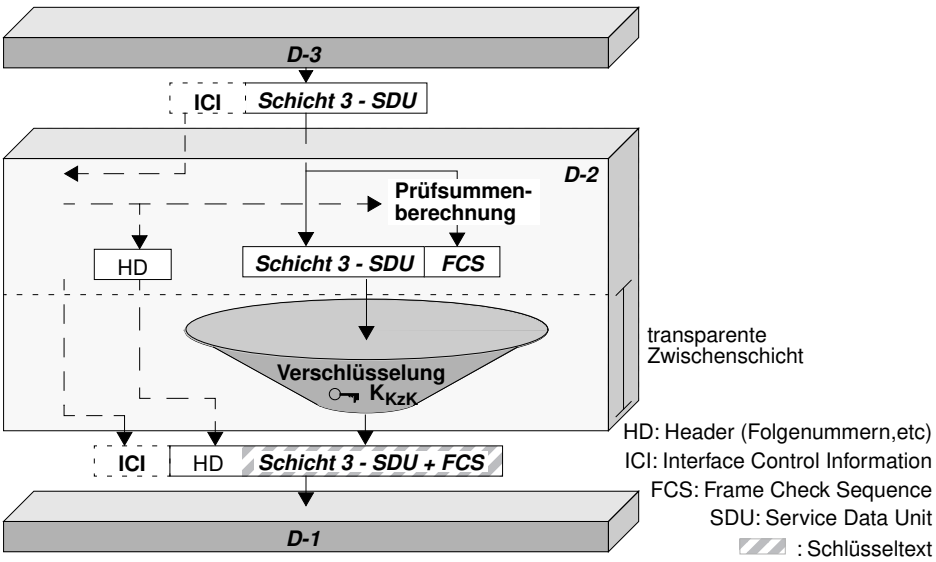


Abbildung 15.12: Verschlüsselung unterhalb der HDLC-Fehlersicherung auf Schicht 2 (KzK_2)

Die so erzeugte Dateneinheit wird normalerweise an Schicht 1 übergeben, welche die Übertragung vorbereitet. Zur Sicherung der Daten gegen aktive Angriffe werden diese vor der Übergabe an Schicht 1 mit dem geheimen Schlüssel K_{KzK} verschlüsselt. Da diese Daten für Schicht 1 transparent sind, entstehen keine Probleme bei der Übergabe dieser verschlüsselten Daten zur Übertragung. Der Header (HD) ist für Schicht 1 nicht transparent und kann im ISDN nicht mitverschlüsselt werden – er steuert beispielsweise über die Schicht 2-Adresse die Priorisierung für gleichzeitig auf den gemeinsamen D-Kanal zugreifende Endgeräte im Teilnehmerbereich. Deshalb werden lediglich die

Schicht 3-SDU und die Prüfsumme verschlüsselt. Der Schicht 2-Header ist durch seine Einrechnung in die Prüfsumme ebenfalls integritätsgeschützt.

Zur eindeutigen Erkennung der Rahmenbegrenzung (01111110) beim Empfänger wird an der Grenze zwischen Schicht 2 und Schicht 1 innerhalb der zu übertragenden Daten nach fünf aufeinanderfolgenden 1en immer ein „0"-Bit eingefügt, welches beim Empfänger wieder entfernt wird. Diese in Abb. 15.12 nicht eingezeichnete Funktion wird durch die vorhergehende Verschlüsselung in ihrer Wirkung nicht beeinflußt.

Die Synchronisierung der kryptographischen Funktionen auf Sende- und Empfangsseite kann sich bei dieser Lösung als aufwendig erweisen, da im Normalbetrieb damit gerechnet werden muß, daß verschlüsselte Daten während der Übertragung verloren gehen. In diesem Fall ist – abhängig vom verwendeten Verschlüsselungsalgorithmus [VoKe_83,DaPr_89] – zusätzlicher Aufwand zur Resynchronisierung der dualen Sicherheitsfunktionen erforderlich. Die Entschlüsselung empfangener Steuernachrichten wird analog zu Abb. 15.12 realisiert.

Alternativ könnte die Verschlüsselung auch am oberen Rand der Schicht 2 realisiert werden. Durch die bekannte Struktur von Schicht 3-Nachrichten ist genügend Redundanz vorhanden, um eine Veränderung des Schlüsseltextes während der Übertragung sicher zu erkennen. Die Integrität von Schicht 2-Protokolldaten wäre dadurch jedoch nicht gewährleistet.

Weitere Kriterien und Randbedingungen für die Allokation von Sicherheitsfunktionen

In Überlegungen zur Plazierung von Sicherheitsfunktionen sind weitere Kriterien einzubeziehen, die vor allem ihre praktische Anwendung und Realisierbarkeit betreffen. Einige solche Kriterien sind:

- Gegebene Vertrauensbereiche bei gemeinsamer Nutzung von Teilnehmeranschlüssen durch verschiedene Teilnehmer (z.B. Unterstützung durch Chipkarten).
- Finanzieller, organisatorischer und administrativer Aufwand für die Realisierung und Leistungsaspekte.
- Aufwand für den Betrieb und das Management der Funktionen:
  - Notwendige Transparenz der Sicherheitsmechanismen gegenüber der Anwendung bzw. Bedienung durch den Nutzer.
  - Verteilung der ausgehandelten Sitzungsschlüssel an die entsprechenden Sicherheitsfunktionen zur Nutzung während der Datenaustauschphase.

  - Aushandlung von Sicherheitsfunktionen und Algorithmen zwischen den Knoten.
  - Synchronisierung der Sicherheitsfunktionen.
- Aufwand für die Wartung der Funktionen:
  - Behebung erkannter Schwächen.
  - Erweiterung bestehender Funktionalität.
  - Anpassung der Schlüssellänge der kryptographischen Funktionen an die erhöhte Rechenleistung moderner Rechner (zur Erhaltung des Aufwandes angenommener Angreifer).
- Notwendige Interoperabilität, Kompatibilität zwischen Knoten (z.B. Endgeräten).

Beim Management der Sicherheitsfunktionen müssen vor allem Sicherheitsparameter, die über die Dauer einer Verbindung hinaus Gültigkeit haben, aktualisiert werden. Im Bereich der Authentikation sind dies z.B. die jeweils gültigen öffentlichen Schlüssel der Kommunikationspartner und Netzknoten zur Signaturprüfung. Diese können innerhalb der Netze periodisch von zentraler Stelle aus an die einzelnen Netzknoten verteilt oder bei Bedarf angefordert werden.

Entsprechende Funktionen innerhalb der Endgeräte sind noch nicht vorgesehen. Die Parameter können z.B. durch die nutzkanalunabhängige Teilnehmer- und Zwischenamtssignalisierung im ISDN angefordert werden bzw. über Funktionen des Intelligenten Netzes [MaPo_96] abgerufen oder verteilt werden.

Auch die Verteilung und Installation der geheimen Signierschlüssel stellt ein noch ungelöstes Problem dar. Das im Aufbau befindliche TMN (Telecommunications Management Network [FaMu_90]) beschreibt ein Netzwerk zum Management von Netzknoten. Ob dieses Netzwerk in der Lage sein wird, Parameter zur Steuerung der Sicherheitsfunktionen von Dienstanbieter bzw. Netzbetreiber sicher (vertraulich und authentisch) über spezielle Netzverbindungen zu den Vermittlungsstellen zu transportieren und dort zu installieren, bleibt fraglich. Eine konventionelle Möglichkeit zur Installation geheimer Schlüssel in die Vermittlungsstellen stellt die manuelle Verteilung dieser Schlüssel durch Mitarbeiter des Netzbetreibers oder Dienstanbieters mit Hilfe von Chipkarten dar. Diese Chipkarten können innerhalb der zugangskontrollierten Vermittlungsstelle an entsprechender Stelle eingefügt und physikalisch gesichert werden. Ein periodischer Austausch müßte dann ebenfalls manuell erfolgen.

Die genannten Randbedingungen, welche eine effiziente Plazierung von Sicherheitsfunktionen beeinflussen, müssen im jeweiligen Anwendungsfall geprüft werden. Technologieabhängige Randbedingungen (z.B. Synchronisierung der kryptographischen Funktionen, hohe Übertragungsraten) und die Abhängigkeit der Betroffenen von am Markt verfügbaren Produkten verbieten allgemein-

gültige Aussagen darüber, wo Sicherheitsfunktionen vorteilhaft implementiert werden können. Vielmehr soll diese Diskussion dazu dienen, eine dem jeweiligen Anwendungsfall entsprechende effiziente Konfiguration zu finden.

15.6 Schlußbemerkung

Die diskutierte Klassifikation von Sicherheitsfunktionen und deren Einordnung in EzE-, KzK- und LzL-Funktionen unterstreicht den Wirkungsbereich von Sicherheitsfunktionen.

Sicherheitsfunktionen sind im allgemeinen nicht transparent für Anwendungen und Netzfunktionen, welche die dadurch geschützten Daten verarbeiten. Die identifizierten Grenzlinien stellen deshalb Schranken dar, außerhalb derer die Transparenz zu schützender Daten für zwischenliegende Netzknoten (bzw. deren Funktionen) nicht garantiert werden kann. Die Grenzlinien beziehen sich nicht ausschließlich auf Schichten, sondern auch auf die Art der zu schützenden Daten. Innerhalb der Schranken, welche durch die Grenzlinien definiert werden, können Sicherheitsfunktionen transparent für zwischenliegende Knoten realisiert werden – damit sind keine Anpassungen in diesen Zwischenknoten notwendig. Dieses gilt nur soweit, wie die Realisierung der Knotenfunktionen der Funktionszuordnung und den Schnittstellenanforderungen des ISO-OSI-Referenzmodelles genügt.

Zum Schutz von sensitiven Daten bieten sich zwei Möglichkeiten:

- Verzicht auf die Daten (Datensparsamkeit)
- aktiver Schutz der Daten (Datensicherheit).

Anwendungsdaten (Nutzdaten) sollten möglichst nahe bei der Anwendung (möglichst weit oben im OSI-RM) geschützt werden, damit der im Vertrauensbereich vorausgesetzte sichere Pfad zwischen Informationsquelle und Sicherheitsfunktion möglichst „kurz“ bleibt, d.h. möglichst wenige – unvollkommene – Funktionen und – unkontrollierte – Übertragungsstrecken enthält. Weiterhin sollten Steuerdaten so nahe wie möglich an der EzE-Grenzlinie (möglichst weit unten im OSI-RM) geschützt werden; dadurch werden auf den Übertragungsstrecken alle Steuerdaten darüberliegender Schichten (z.B. Adressen) geschützt.

Zusätzlich sind LzL-Funktionen zur Realisierung von Grundsicherheit innerhalb des Netzes und im Teilnehmeranschlußbereich notwendig. Damit können Daten auch dann auf den Übertragungsstrecken geschützt werden, wenn sie nicht für die zwischen den Endgeräten lokalisierten Netzknoten transparent sind.

Redundante Sicherheitsfunktionen bieten ergänzenden Schutz beim Ausfall einzelner Sicherheitsfunktionen und erhöhen die Kompatibilität durch die Mög-

lichkeit der Aushandlung kompatibler dualer Sicherheitsfunktionen zwischen verschiedenen Knoten.

Literatur

ATMF_97 The ATM-Forum Technical Committee: „Phase I ATM Security Specification (Draft)“, ATM Forum BTD-Security-01.02, April 1997

BaGo_95 G. Bandow, H. Gottschalk, D. Gehrmann, W. Hlavac, H. Koch, W. Müller, D. Schwetje: „Zeichengabesysteme - Eine neue Generation für ISDN und intelligente Netze“, L.T.U. - Vertriebsgesellschaft mbH, Bremen, 2. Auflage, 1995

Blab_95 A. Blab: „Hoher Sicherheitsstandard bei Hicom“, siemens telcom report 18, 5/1995, pp. 259-261

Chau_81 D. Chaum: „Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms“, Communications of the ACM 24/2 (1981) 84-88

DaPr_89 D. W. Davies, W. L. Price: „Security for Computer Networks“, 2nd ed., Wiley series in communication and distributed systems, 1989

Engb_93 R. O. M. Engberding: „Spionageziel Wirtschaft“, VDI-Verlag, 1993

FaMu_90 R. Falkner, H. Müller: „Telecommunications Management Network (TMN): Architektur, Schnittstellen und Anwendungen“, ntz, Bd. 43, Heft 6, 1990, pp. 466-469

GSM1_93 ETSI: „GSM Recommendations: GSM 01.02 - 12.21“, February 1993, Release 92

GSM2_89 ETSI: ETSI/TC GSM: „06.10 GSM full rate speech transcoding; Version 3.2.0“, July 1989

GSM3_92 ETSI: ETSI/TC GSM: „06.20 GSM Digital Speech Compression“, Version 4.0.0; 1992

ISO1_89 ISO 7498-2 International Standardization Organisation: „Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture“, 1989

ISO2_89 ISO 7498 International Standardization Organisation: „Basic Reference Model for Open Systems Interconnection“,1989

KeFe_96 D. Kesdogan, H. Federrath, A. Jerichow, A. Pfitzmann: „Location Management Strategies increasing Privacy in Mobile Communication Systems“, in: Information Systems Security. Facing the information society of the 21st century. Proc. of the IFIP SEC '96 12th International Information Security Conference 21 - 24 May, 1996, Greece, Chapman & Hall, 1996

LaAh_86 Y. Lapid, N. Ahituv, S. Neumann: „Approaches to Handling „Trojan Horse“ Threats“; Computers & Security, 5, North-Holland, 1986, pp. 251-256

Mant_91 R. Manterfield: „Common Channel Signalling“, IEEE Communications Series 26, Peter Peregrinus Ltd., 1991

MaPo_96 T. Magedanz, R. Popescu-Zeletin: „Intelligent Networks - Basic Technology, Standards and Evolution“, International Thomson Computer Press, 1996

Muel_96 J. Müller: „Realisierungsmöglichkeiten von Ende-zu-Ende-Vertraulichkeit in GSM-Mobilfunknetzen“, Großer Beleg, TU Dresden, Institut für Theoretische Informatik, April 1996

Nitz_95 J. Nitz (Hrsg.): „Lauschangriff - Das Buch zur Wanze“, edition ost, scripton hannover, Berlin 1995

Pfit_90 Andreas Pfitzmann: „Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz“, IFB 234, Springer-Verlag, Heidelberg 1990

Pfit_95 A. Pfitzmann: „Datensicherheit und Kryptographie“, Skriptum zur gleichnamigen Vorlesung, Technische Universität Dresden, Fakultät für Informatik, 1995

PfPf_95 A. Pfitzmann, B. Pfitzmann, M. Schunter, M. Waidner: „Vertrauenswürdiger Entwurf portabler Benutzerendgeräte und Sicherheitsmodule“, Proc. Verläßliche Informationssysteme (VIS' 95), Vieweg, 1995

Pohl_95 N. Pohlmann: „Schutz von LANs und LAN-Kopplung über öffentliche Netze“, DATACOM, 6, 1995, pp. 50-56

Q9xx_89 CCITT Q.930-Q.940: „Digital Subscriber Signalling System No. 1 (DSS1), Network Layer, User-Network Management“, Recommendations Q.930-Q.940, Geneva, 1989

RiSh_78 R. L. Rivest, A. Shamir, L. Adleman: „A Method for Obtaining Digital Signatures and Public-Key Cryptosystems“, Communications of the ACM, Volume 21, No. 2, Feb 1978, pp. 120-126

Sail_96 R. Sailer: „Integrating Authentication into Existing Protocols“, Proc. of the 5th Open Workshop On High Speed Networks, Paris, March 20-21, 1996, pp. 4.25 - 4.31

SaRe_84 J. Saltzer, D. Reed, D. Clark: „End-To-End Arguments in System Design“; ACM Transactions on Computer Systems, Vol. 2, No. 4, November, 1984, pp. 277-288

Sieg_92 G. Siegmund: „Grundlagen der Vermittlungstechnik“, R. v. Decker, 1992

VoKe_83 V. L. Voydock, S. T. Kent: „Security Mechanisms in High-Level Network Protocols“, Computing Surveys, Vol. 15, No. 2, June, 1983, pp. 135-171