Sichere Datenkommunikation Teil II

von Prof. Dr.-Ing.
Bernhard Walke, Iserlohn

Viele der im ersten Teil dieses Beitrags (KES 5/85) aufgezählten Gefahren gehen von Menschen aus und erfordern entsprechend intelligente Vorbeugemaßnahmen. Andere Gefahren ergeben sich deshalb, weil Datenverarbeitung und -übertragung mit elektrotechnischen Einrichtungen erbracht werden (technisches Versagen, höhere Gewalt). Solange kein Netz zwischen den beteiligten Datenendeinrichtungen (DEE) liegt oder nur die Übertragungsphase (zwischen Verbindungsauf- und -abbau) in LV-Netzen betrachtet wird, reichen die bekannten Verschlüsselungs- und Codierverfahren völlig aus. Sonst kommt der Problemkreis der sicheren Vermittlung mit seinen Forderungen an die Betriebssoftware der Kommunikationsprozessoren hinzu.

Schwachstellen bei PV-Netzen . . .

Schwachstellen für eine sichere Übermittlung über PV-Netze bilden

- Interfaces (die Schnittstellen können falsch benutzt werden),
- Protokolle (die Regeln werden u. U. nicht eingehalten),
- Funktionseinheiten (die Funktionen werden u. U. nicht korrekt erfüllt).

. . . und Maßnahmen zur Erhöhung der Sicherheit

Wir betrachten nachfolgend Maßnahmen zur Erhöhung der Sicherheit von Übertragungswegen und von Betriebssoftware der Kommunikationsprozessoren. Maßnahmen zur Förderung der Sicherheit von Kommunikationsprozessoren sind auch für Hosts mit sicherheitsrelevanter Verarbeitung anwendbar und in drei Gruppen einzuteilen:

- Bereitstellung sicherer Funktionseinheiten (Verifikation ihrer korrekten Arbeitsweise),
- Verifikation von Kommunikationsprotokollen in Bezug auf korrekte und sichere Funktionsweise,
- Isolierung von Systemteilen/Komponenten, Schichten und Funktionseinheiten und Einsatz von Schutzmechanismen zur Zugriffsüberwachung.

Lösungsansätze nach dem heutigen technischen Stand

Gemäß Bild 3[1)] sind *Rechensysteme* und ihre Perpherie sowie die *Übertragungswege* als sicherheitsempfindliche Bereiche anzusehen. Für beide Bereiche gibt es wirksame Mittel zur Erhöhung der Sicherheit, wie nachfolgend beschrieben wird.

Man unterscheidet *organisatorische Maßnahmen* für den Aufbau und Betrieb der Kommunikationsrechner (bzw. Hosts) und *formale Entwicklungsmethoden* für ihre Betriebssoftware. Beides zusammen trägt zu einem kalkulierbaren kleinen Sicherheitsrisiko der Systeme bei.

Organisatorische Maßnahmen

Das älteste bewährte Verfahren ist die *Zugangskontrolle* zu sicherheitsempfindlichen Systemen, ihren Daten und dem Aufstellungsort überhaupt. Dazu gehören die z. T. bekannten Abläufe bei Zugriff auf Leistungen eines Rechners, z. B. beim „Einloggen" die Phasen

— Identifizierung (für Verwaltungszwecke),
— Authentisieren (Nachweis, daß man der vorgegebene Teilnehmer ist, Paßwort),
— Autorisierung (vom System für den Zugang zu bestimmten Programmen und Daten).

Sicherheitspolitik

Eine weitere bewährte zusätzliche Methode ist die Anwendung einer *Sicherheitspolitik* für das gesamte System und seine Benutzer. Sie legt die Zugangsregeln zu Programmen und Daten fest und hat folgende wesentliche Komponenten:

— Einstufung (classification) von Information, zur Verhinderung unberechtigter Einsichtnahme oder Veränderung.
— Vergabe von Berechtigungen für Benutzer zur eindeutigen Abgrenzung zwischen Benutzern mit Zugangsrechten zu unterschiedlich eingestuften Daten.
— Festlegung der Zugangsregeln von Benutzern zu Code und Daten.

[1)] siehe KES 5/85, S. 186

Sinn der Abgrenzung

Diese Technik ist allgemein üblich und soll beispielsweise verhindern, daß ein Angestellter der Personalabteilung Einfluß auf den Inhalt von Anwendungsprogrammen der Entwicklungsabteilung einer Firma, oder ein Entwicklungsingenieur Einblick in die Gehaltskonten seiner Kollegen erhält, die auf demselben Rechensystem verfügbar sind. Die Tatsache, daß in sehr vielen Fällen Personal- und Entwicklungsabteilungen physikalisch getrennte Rechner benutzen, läßt das große Mißtrauen gegen die Realisierbarkeit einer geeigneten Sicherheitspolitik bereits ahnen.

Sicherheit durch Stufenbetrieb

Die Sicherheit eines Rechensystems kann noch weiter durch *Stufenbetrieb* erhöht werden:
Einstufenbetrieb liegt vor, wenn eine Rechenanlage nur Programme und Daten einer Sicherheitsstufe speichert und verarbeitet.
Mehrstufenbetrieb dagegen verlangt innerhalb des Rechnersystems Vorsichtsmaßnahmen, um die Verletzung von Sicherheitsregeln zu verhindern. Zwei Betriebsweisen werden hier unterschieden:

Bei Höchststufenbetrieb müssen alle Benutzer die Berechtigung zum Zugang auch der am höchsten eingestuften im System vorhandenen Daten haben, selbst wenn sie nicht direkt mit diesen Daten arbeiten. Es wird dabei unterstellt, daß das System fehlerhaft ist und nicht die saubere Trennung bei der Speicherung und Verarbeitung verschieden eingestufter Programme und Daten garantieren kann.

Periodischer Stufenbetrieb

Im periodischen Einstufenbetrieb wird das gleiche Rechensystem, z. B. vormittags für den Einstufenbetrieb von Daten der Stufe „geheim", nachmittags für „offene" benutzt. Zwischen diesen beiden Betriebsphasen muß eine Phase zwischengeschaltet werden, in der
— Datenträger ausgetauscht,
— Hauptspeicher und Register gelöscht,
— Farbbänder ausgewechselt werden,
— das Betriebssystem neu generiert wird.

Es ist unmittelbar einsichtig, daß diese Betriebsweisen auch zur sicheren Trennung gleich wichtig eingestufter, aber dennoch verschiedenen Benutzern vorbehaltener Daten anwendbar sind, z. B. für Personal- und Entwicklungsabteilung.

hter Mehrstufenbetrieb . . .

Kommunikationsprozessoren können nicht in einem der bisher genannten Formen des Stufenbetriebs, sondern nur im sogenannten *echten Mehrstufenbereich* betrieben werden. Diese Betriebsart hat folgende Merkmale:
— konkurrierende Bearbeitung verschieden eingestufter Information durch Benutzer verschiedener Berechtigung.
— der Rechner garantiert die erforderliche saubere Trennung der Information.

Echter Mehrstufenbereich erfordert ein vertrauenswürdiges Betriebssystem mit
— Schutz-Eigenschaften, die eine effiziente Zugriffsüberwachung beinhalten,
— Zusicherung vollständiger und korrekter Beachtung aller realisierten Kontrollen.

. . . bei Kommunikationsprozessoren

Bei Kommunikationsprozessoren tritt echter Mehrstufenbereich immer dann auf, wenn unterschiedlich eingestufte Daten (z. B. verschiedener Teilnehmer) vermittelt werden müssen. Der Vermittlungsvorgang beinhaltet als Kernfunktion das Weiterleiten von auf einer Leitung ankommenden Daten auf eine abgehende Leitung.

Im Falle der Leitungsvermittlung muß sichergestellt werden, daß Datenquelle (hinter der Eingabeleitung) und Datensenke (hinter der Ausgabeleitung)

Einstufung durch Datenendeinrichtungen

nicht nur logisch zu einer Verbindung gehören, sondern auch beide die Berechtigung zum Empfang der übertragenen Daten besitzen. Die entsprechenden Authentisierungs- und Autorisierungsfunktionen sind Teil der sogenannten höheren Ebenenprotokolle der Datenendeinrichtungen, meistens der Sitzungs- oder Anwendungssteuerung. Sie betreffen also nicht das Transportsystem und seine Vermittlungen. Es stellt *lediglich die geschalteten Verbindungen zur Verfügung.*

Keine Differenzierung im PV-Netz

Im Fall der Paketvermittlung folgen auf einer Eingabeleitung des Kommunikationsprozessors aufeinander Pakete verschiedener logischer Verbindungen mit unterschiedlicher Einstufung der enthaltenen Daten. Hier erfolgt die Vermittlung entsprechend dem Speichervermittlungsprinzip. Die Daten werden also zwischengespeichert, so daß unterschiedlich eingestufte Daten im Hauptspeicher liegen können. Aus den Paketköpfen ersieht der Kommunikationsprozessor, wohin das Paket zu vermitteln ist.

Während der Datenteil verschlüsselt bleiben könnte, muß der Paketkopf im Vermittlungsverfahren offen (im Klartext) vorliegen. Es ist klar, daß die Vermittlungen und Betriebssystem-Programme korrekt mit den Paketen umgehen müssen, um keine sicherheitsrelevanten Fehler zu begehen oder solche vielleicht anderen Programmen zu ermöglichen. Bisher ist kein Verfahren akzeptiert, das eine sichere Ende-zu-Ende (Quelle-Senke)-Verschlüsselung ermöglicht. Deshalb sind auch verschlüsselte Datenteile von Paketen im Vermittlungsrechner so wie offene zu behandeln. Selbst wenn ein Verfahren akzeptiert wäre, bleibt das Risiko des absichtlichen Fehlleitens von Paketen (denial of service) durch die Vermittlungssoftware, so daß gleich hohe Sicherheitsforderungen erhoben werden müssen wie für Hostsysteme.

Vermittlungsrechner muß Berechtigung verifizieren

Schließlich ist es — wie bei Leitungsvermittlungsnetzen — Aufgabe des Vermittlungsrechners zu verifizieren, daß ein Empfänger die vorgegebene Berechtigung tatsächlich auch hat.

Jedes im echten Mehrstufenbetrieb arbeitende System verknüpft mit jedem Benutzer eine Berechtigung (die es in einem Identifikations- und Authentisierungsprozeß verifiziert hat) und behandelt jede gespeicherte Information (Befehle und Daten) entsprechend einer vom Benutzer oder anderen autorisierten Personen angegebenen Einstufung.

Grundforderungen an ein sicheres Netz . . .

Als Grundforderungen an ein sicheres Rechnernetz sind zu nennen
— Ausschluß nicht autorisierter Benutzer (Terminals)
— Verhütung des Ausschlusses autorisierter Benutzer,
— Garantie der Integrität der übermittelten Nachrichten,
— Verhütung des Entzugs von Dienstleistungen (denial of service),
— Schutz des Netzüberwachungs- und Verwaltungsverkehrs.

Dieselben Forderungen gelten auch bezüglich Rechenzentren (Hosts) mit oder ohne Zugang der Benutzer über Terminals.

. . .und die dafür notwendigen Voraussetzungen

Der Sicherheitsanspruch des Kommunikationsnetzes stützt sich auf die folgenden Forderungen und Voraussetzungen:
— Einführung eines allgemein gültigen Kennzeichnungssystems, um die Einstufung von Daten und Berechtigungen von Benutzern festzulegen (z.B. Benutzergruppe).
— Festlegung einer Sicherheitspolitik, um den Zugang von Benutzern zu Daten zu regeln.
— Kennzeichnung aller durch das Netz übertragenen Daten durch Sicherheitsstufen.
— Garantie der Datenintegrität und des Einstufungskennzeichens der Daten.
— Einführung von Berechtigungen für Hosts, um die Einstufung von Daten anzugeben, die ein Host senden/empfangen darf.

Verantwortung beim Netz

— Garantie, daß jeder Host nur Daten empfängt/sendet, die seiner Berechtigung entsprechen (falls der Host verschieden eingestufte Daten besitzen darf, ist er für die Integrität der Einstufungsmerkmale und der Daten gegenüber dem Netz verantwortlich).

Das Netz (also die Kommunikationsrechner), ist dafür verantwortlich, daß alle Einstufungskennzeichen und Daten unverändert übertragen werden.

Formale Entwicklungsmethoden für sichere Kommunikationsprozessoren

Die Grundprinzipien für eine sichere Verarbeitung sind in [1][2] dargestellt. Man benötigt sog. ,,vertrauenswürdige'' Software, die einem aufwendigen Verifikationsprozeß unterworfen wurde und dadurch als korrekt im Sinne ihrer Spezifikation gelten darf. Auch benötigt man heute noch nicht allgemein übliche Hardwareeigenschaften der Kommunikationsrecher, ohne die ein echter Mehrstufenbetrieb wirtschaftlich nicht realisierbar ist [1].

Sichere Übertragungswege

Datenkommunikation über Fernnetze (z. B. Bild 2[3]) führt in der Regel dazu, daß die betroffenen Teilnehmer nicht unmittelbar, sondern über mehrere sequentielle Teilstrecken unter Zwischenschaltung von Kommunikationsprozessoren miteinander verbunden sind. Fragen der Netzsicherheit, soweit sie durch Maßnahmen in diesen Prozessoren beeinflußbar sind, wurden bereits besprochen.

Zur Sicherung der Übertragungswege setzt man einerseits die bekannten Codierverfahren zur Fehlererkennung und Korrektur von Übertragungsfehlern und andererseits die Datenverschlüsselung ein. Dabei unterscheidet man zwischen Leitungs- und Ende-zu-Ende Verschlüsselung.

Leitungsverschlüsselung

Leitungsverschlüsselung hat heute einen so hohen technischen Stand, daß man (mit entsprechendem Aufwand) eine fast beliebig hohe Sicherheit bei der digitalen Datenübertragung erreichen kann [5].
Bei Anwendung der Leitungsvermittlungstechnik ist es technisch möglich, nach ihrem Aufbau die dann als Kanal realisierte Verbindung zwischen den Teilnehmern verschlüsselungstechnisch als eine physikalische Leitung zu behandeln, so daß mit Leitungsverschlüsselung ein sicherer Übertragungsweg zwischen Datenquelle und -senke garantiert werden kann.

Bei Anwendung der Paketvermittlungstechnik können die Vorteile der Leitungsverschlüsselung nur auf jeder Teilstrecke zwischen den Kommunikationsprozessoren genutzt werden. Die Prozessoren benötigen, wie schon erläutert, auch in der Übertragungsphase einer Verbindung Daten aus den Paketen, um ihre Vermittlungsaufgabe zu erfüllen. Da nun Kommunikationsprozessoren bisher nicht dafür ausgestattet sind, einen echten Mehrstufenbetrieb sicher durchzuführen, müssen andere Maßnahmen ergriffen werden, um diesen Sicherheitsmangel wettzumachen. Dafür kommt als einzige Möglichkeit die Ende-zu-Ende Verschlüsselung in Betracht.

Ende-zu-Ende-Verschlüsselung (EZE-V)

Entsprechend dem US-Standard FED-STD-1026 (Draft 2) sind fünf Sicherheitsziele zu beachten, die alle die Kompatibilität der Kommunikationspartner voraussetzen (deshalb ist ein EZE-V-Standard nötig):

1.) Verhütung der Enthüllung von Klartext-Nachrichten,
2.) Erkennung der betrügerischen Veränderung einer Nachricht,
3.) Erkennung der betrügerischen Einfügung einer Nachricht,
4.) Erkennung der betrügerischen Zerstörung einer Nachricht,
5.) Erkennung der Wiederholung einer früher gültigen Nachricht.

Es wird ein EZE-Standard angestrebt, der diese 5 Bedrohungen beseitigt und doch den Verkehr von Endgeräten verschiedener Hersteller untereinander zuläßt.

---

[2] siehe Literaturverzeichnis
[3] siehe KES 5/85, S. 185

Erweiterung der Kommunikationsregeln

Die Datenkommunikation zwischen Partnern folgt in jedem Einzelfall einem bestimmten Regelwerk (Satz von Protokollen), das Steuersignale, Formate, Meldungslängen, Optionen usw. festlegt und damit Syntax und Semantik des Kommunikationsablaufs bestimmt.

Um die speziellen Anforderungen der Ende-zu-Ende-Verschlüsselung in dieses Regelwerk zu integrieren, müssen dort vorhandene Funktionen erweitert werden. Diese Funktionen lassen sich entsprechend dem Architekturmodell der ISO logisch gliedern. Dabei sind die Verschlüsselungsmaßnahmen in die entsprechenden Ebenenprotokolle des ISO-Modells zu integrieren.

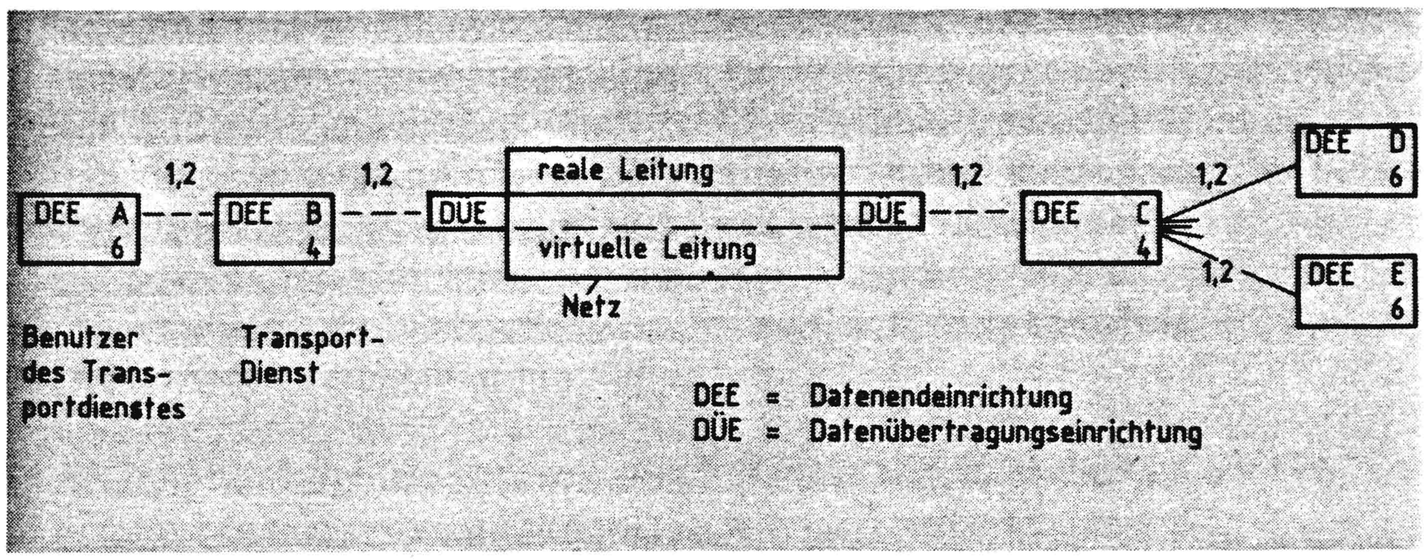

Bild 4: Verteiltes System mit Datenübertragung. Die Zahlen in den Datenendeinrichtungen (DEE) und Datenübertragungs-Einrichtungen (DÜE) geben an, in welcher Ebene des ISO-Modells jeweils verschlüsselt wird

Verschlüsselungsarten

Entsprechend Bild 4 und Bild 5 unterscheidet man Leitungs-, Kanal-, Transport- und EZE-Verschlüsselung. Leitungs- oder Kanal-Verschlüsselung wird eingesetzt, wenn physikalische Leitungen bzw. Multiplexleitungen zwischen Punkt-zu-Punkt- oder Mehrpunktverbindungen verwendet werden. Die Leitungen können privat oder Bestandteil öffentlicher Netze sein. Transport-Verschlüsselung wird zum Schutz virtueller Verbindungen in PV-Netzen zwischen den Datenendeinrichtungen (DEE) eingesetzt, wobei viele Leitungsabschnitte enthalten sein können.

EZE-V schützt den Nachrichtenaustausch zwischen Anwendungen in verschiedenen Prozessoren; z. B. sind in Bild 4 DEE A ein Host, DEE B der zugehörige Kommunikationsrechner, DEE C eine Multiplex-Einrichtung für Terminals und DEE D bzw. E abgesetzte Terminals. Die Verschlüsselung von Daten der Ebene 6 schützt dagegen, daß DEE B bzw. DEE C Daten (un)beabsichtigt vertauschen und damit die Datensicherheit verletzen [2].

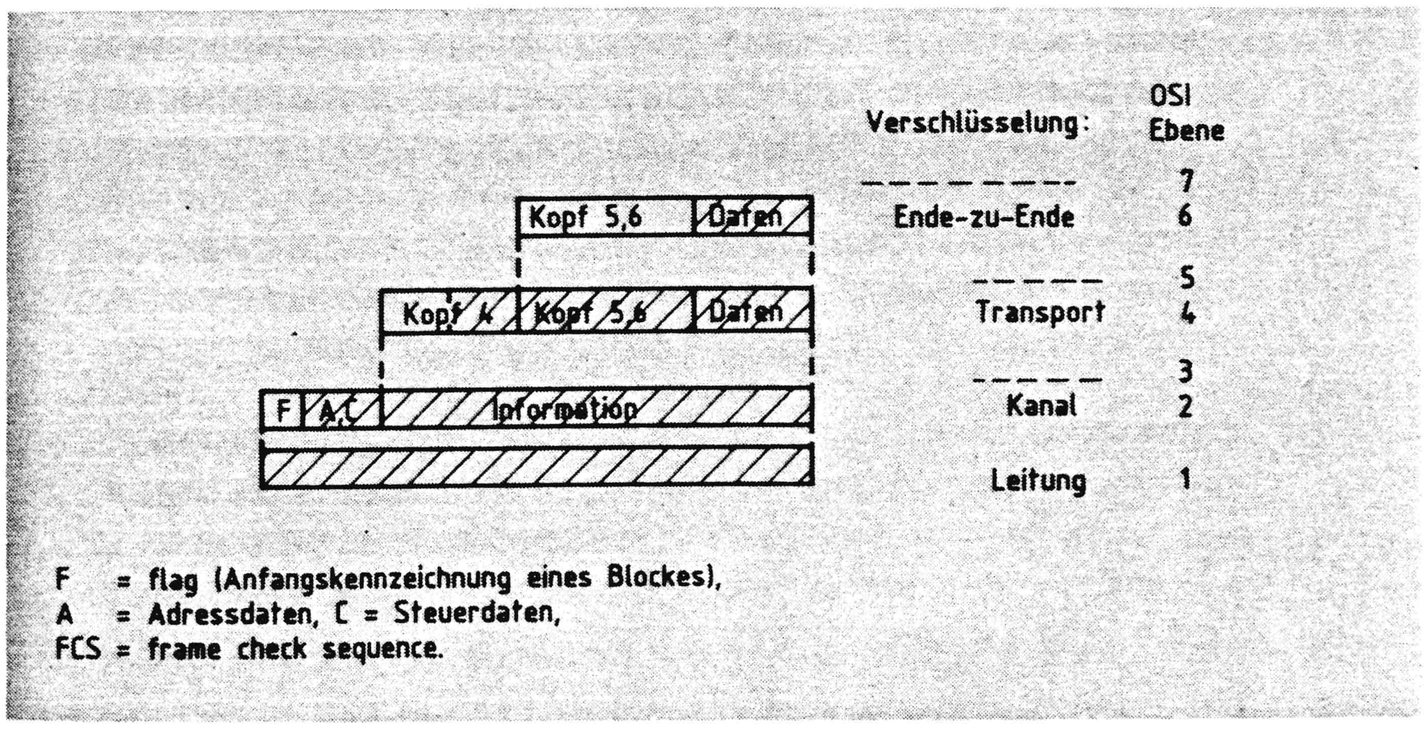

Bild 5: Aufsatzpunkte für Verschlüsselung im OSI-(Open System Interconnection) Architekturmodell der ISO. Schraffierte Daten werden in der entsprechenden Ebene verschlüsselt.

Aus Bild 5 ist zu sehen, wie auf der Sendeseite mit zunehmender Aufbereitung für die Übertragung von Daten ausgehend von der Ebene 7 (Verarbeitung), Adreß- und Steuerinformationen in den Ebenen 6 bis 2 zugefügt wer-

Verschlüsselungsregeln

den und welche Daten jeweils verschlüsselt werden dürfen. Die offen verbliebenen Daten werden jeweils von der darunter liegenden Ebene, die evtl. in einem separaten Gerät realisiert ist, benötigt, um arbeiten zu können.

Beispielsweise übergibt sendeseitig Ebene 2 ihre HDLC-Blöcke mit unverschlüsselten Flags an Ebene 1 und erkennt sie empfangsseitig an diesen Flags (Flags sind geschützte Bitfolgen, sechs 1-Bits).

Sichere Übertragung bei PV . . .

EZE-V befaßt sich wegen ihrer Anwendungsnähe mehr mit ,,Information'' als mit ,,Kommunikation'', jedoch bestehen in der Vorgehensweise große Ähnlichkeiten zwischen Transport- und EZE-Verschlüsselung. Man erwartet deshalb die Entwicklung sehr ähnlicher Standards für beide Bereiche (vgl. [3]). Heute existierende offene PV-Netze übertragen, was immer die DEE an der Netzschnittstelle anliefern, z. B. auch EZE-verschlüsselte Daten, die im Datenteil der Pakete vorliegen. Es scheinen also alle Sicherheitsprobleme der Datenübertragung auch bei PV gelöst zu sein.

. . . mit Einschränkungen

Die Technik der EZE-V wird, wenn sie einmal standardisiert und eingeführt ist, nur einen Teil der Sicherheitsproblematik von PV-Netzen lösen können, nämlich garantieren, daß zwei Teilnehmer ihre Daten unverfälscht und unbeobachtet übertragen können. Ein für alle Typen von vermittelnden Datennetzen wichtiger zweiter Aspekt, nämlich die Garantie der Sicherheit des Gesamtnetzes, kann erst dann als befriedigend gelöst angesehen werden, wenn auch sichere Kommunikationsprozessoren verfügbar sind. Dementsprechend müssen sowohl Leitungs- als auch Paketvermittlungsnetze als unsicher angesehen werden.

Aber selbst private Netze sind häufig unsicher

Sicherheitsempfindliche Behörden/Organisationen verwenden für ihre Aufgaben private Datennetze, die durch hohen technischen Aufwand sicherer als offene Netze gemacht worden sind. Dies ist in der Tat der Grund dafür, daß es z. B. viel mehr private als offene PV-Netze gibt. Gemessen an den eben dargestellten Forderungen zur Gewährleistung von sicherer Datenkommunikation sind jedoch fast alle diese privaten Netze als unsicher einzustufen, denn sie sind nicht entsprechend den neueren sicherheitstechnischen Möglichkeiten ausgestattet (vgl. die in [1] zusammengestellten Forderungen an solche Netze). Der heutige sicherheitstechnische Stand erlaubt es nicht, alle bekannten Risiken durch kostengünstige Gegenmaßnahmen abzuwenden.

Hoffnung für die Zukunft

Beispielsweise ist der Korrektheitsnachweis von großen Vermittlungsprogrammen heute noch weitgehend von Hand, mit noch unzureichender Unterstützung durch z. Zt. erst in Entwicklung befindliche Programme, möglich. Es gibt jedoch berechtigte Hoffnungen auf die Verfügbarkeit solcher ,,Tools'' für die Produktion sicherer Software in den nächsten Jahren.

Literatur:

[1] Walke B.: Software-Aspekte sicherer Datenkommunikation. Elektron. Rechenanl. 25, 170 (1983)
[2] Elden W. L.: Proposed ANSI level 4 transport encryption standard. Proc. Nat. Telecomm. Conf. '79, p. 32.41
[3] Proposed Federal Standard 1025: Telecommunications: Interoperability and security requirements for use of the data encryption standard in the network and transport layers of data communications, June 1, 1981
[4] Department of Defense Directive 5200.28 M ,,Techniques and Procedures for Implementing, Deactivating, Testing and Evaluating Secure Resource Sharing ADP Systems'', June 1979
[5] Popek, G. J., Kline C. S.: Encryption and secure computer network. Comput. Surv. 11,331 (1979)

KES 6/85 — Postfach 1368 — D-6507 Ingelheim