R. Sailer, P. Kühn:„Ein Domain-Konzept zur systematischen und wirtschaftlichen Integration von Sicherheit in Kommunikationsnetze“, *it + ti Informationstechnik und Technische Informatik*, 38. Jahrgang, Heft 4, 1996, pp. 30-33

Ein Domain-Konzept zur systematischen und wirtschaftlichen Integration von Sicherheit in Kommunikationsnetze

R. Sailer, P. J. Kühn

1 Einleitung

Die Kommunikationstechnik bietet heute viele Dienste an, die für die wirtschaftliche Leistungsfähigkeit eines Unternehmens eine zunehmend wichtige Rolle spielen. Da die Investitionen in die Kommunikationsinfrastruktur enorm sind, müssen die Ressourcen als Basis bestehender und neuer Dienste längerfristig genutzt werden. Gleichzeitig sind die Anforderungen an die Sicherheitsaspekte gestiegen, welche oftmals bei der Einführung neuer Systeme und Dienste noch nicht konkretisiert werden können und deshalb nur unzulänglich Berücksichtigung finden.

In diesem Zusammenhang werden Möglichkeiten zur additiven Integration von Sicherheit in bestehende Kommunikationsnetze untersucht. Da Sicherheit in heute verfügbaren Anwendungen nur unzureichend integriert ist, streben wir an, die Kommunikationsinfrastruktur mit Sicherheitsfunktionen anzureichern. Dabei werden schützenswerte Daten auf ihrem Weg durch das Kommunikationsnetz gesichert. Der verbleibende Freiraum für Angriffe zwischen der eigentlichen Verarbeitung der Daten und dem Wirkungsbereich der integrierten Sicherheitsfunktionalität wird durch Zugangs- und Zugriffskontrollmechanismen eingeschränkt.

Abschnitt 2 beschreibt die Kopplung von Lokalen Netzen über öffentliche Kommunikationsnetze. Diese Konfiguration wird in Abschnitt 3 schrittweise unter Anwendung eines vorgestellten Konzeptes mit Sicherheitsfunktionalität angereichert. Im Ausblick werden weiterführende Arbeiten am vorgestellten Konzept motiviert.

2 Beispiel-Konfiguration

Dieser Abschnitt beschreibt eine Konfiguration zur Kopplung verschiedener Lokaler Netze (Local Area Networks, LANs) über öffentliche Kommunikationsnetze. Das in Bild 1 dargestellte Signalisiersystem transportiert Nachrichten, die zur Steuerung der Vermittlungseinrichtungen des Netzes notwendig sind. Die jeweiligen Netzbetreiber nehmen die zur Verbindung der Lokalen Netze über das öffentliche Kommunikationsnetz (z.B. ISDN,

B-ISDN/ATM) notwendigen Einstellungen über das Netzmanagement und die Administration vor.

Mit dem Dienst *Virtuelles Privates Netz* (Virtual Private Network, VPN) können verschiedene, räumlich weit getrennte LANs zu einem übergreifenden logischen LAN zusammengefaßt werden. Beispielsweise können auf der Konfiguration in Bild 1 aufbauend die LANs räumlich getrennter Niederlassungen eines Unternehmens über den Dienst *VPN* logisch zu einem Unternehmensnetz zusammengefaßt werden. Da die zur Realisierung eines VPNs genutzten öffentlichen Netze nicht vom Unternehmen kontrolliert werden können, muß dort mit umfassenden Angriffsmöglichkeiten gerechnet werden [1].

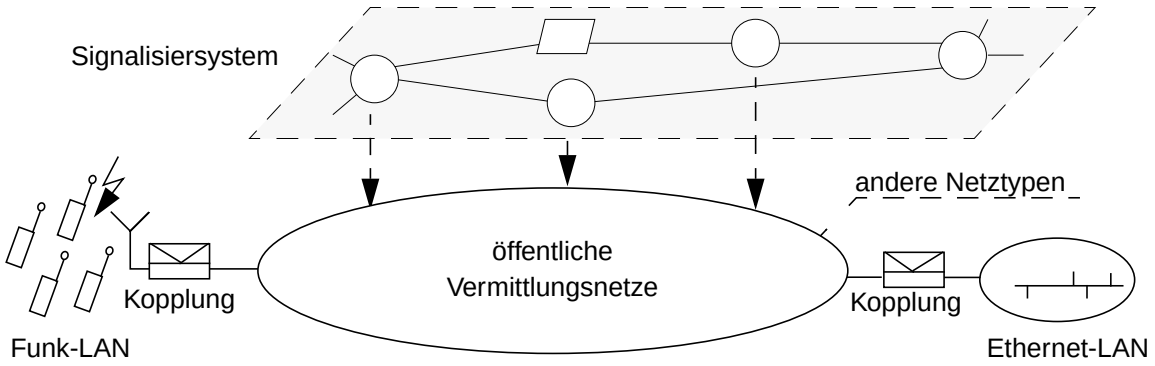

Bild 1: Kopplung von LANs über öffentliche Kommunikationsnetze

Wir werden uns im folgenden auf die Sicherung der Information konzentrieren, die in Form von Nutzdaten in den LANs verarbeitet wird. Im Beispiel des *VPNs* eines Unternehmens können dies Forschungs- und Entwicklungsdaten oder Buchhaltungsinformation sein. Die Anforderungen aus Sicherheitssicht an die Verarbeitung und Haltung solcher Daten sind: (i) *Vertraulichkeit*, (ii) *Integrität*, (iii) *Verfügbarkeit*. (i) verhindert das Ausspionieren von wichtigen, geheimen Daten durch konkurrierende Unternehmen. (ii) verhindert das unbemerkte, unautorisierte Verändern von Daten und (iii) ist Voraussetzung für die wirtschaftliche Leistungsfähigkeit eines von diesen Daten permanent abhängigen Unternehmens. Die Sicherheitsanforderungen (i) bis (iii) bezogen auf die oben genannten schützenswerten Daten werden im folgenden als *Schutzziele* bezeichnet.

Das im folgenden Abschnitt vorgestellte Domain-Konzept kann als Wegweiser dienen für die Vorgehensweise bei der Integration von Mechanismen zur Realisierung der genannten Sicherheitsanforderungen.

3 Das Domain-Konzept am Beispiel VPN

Ein Domain ist eine Partition einer untersuchten Konfiguration, in der bestimmte Schutzziele einheitlich realisiert werden können.

Ein Domain ist dadurch charakterisiert, daß in ihm jeweils einheitliche

- Angriffsmöglichkeiten bezüglich schützenswerter Objekte,
- technische und organisatorische Gegebenheiten,
- Schutzziele,
- Zuständigkeiten und Verantwortlichkeiten für Management, Administration und Organisation

herrschen.

Ein Domain wird im folgenden als *sicher* bezeichnet, falls alle zugehörigen Schutzziele innerhalb dieses Domains erfüllt werden.

Im Rahmen der Anwendung des Domain-Konzeptes auf ein VPN ist in einem ersten Schritt eine Verfeinerung der Konfiguration notwendig. Durch die Abbildung der physikalischen und logischen Systemkonfiguration auf hinsichtlich der genannten Kriterien unterscheidbare Domains können die einzubringenden Sicherheitsmechanismen an die jeweiligen *Gegebenheiten* angepaßt werden. Außerdem können auf die jeweilige Umgebung zugeschnittene Sicherheitsmaßnahmen ergriffen werden, um *Angriffsmöglichkeiten* zu begegnen, die ebenfalls von den logischen und physikalischen Gegebenheiten des zu sichernden Domains abhängen. Fehlende Angriffsmöglichkeiten, z. B. weil bestimmte Angriffspunkte für angenommene Angreifer fehlen, können den Aufwand für die Realisierung von Schutzzielen für bestimmte Domains reduzieren.

Ebenso können *Schutzziele* völlig entfallen, falls die zugehörigen schützenswerten Daten innerhalb des betrachteten Domains nicht ungeschützt vorliegen.

Schließlich müssen die einzubringenden Sicherheitsmechanismen auch verwaltet werden. Es müssen aktuelle Software-Versionen installiert, Zugriffsrechte gesetzt, Schlüssel verwaltet und Überwachungsergebnisse (z. B. Log-Dateien) interpretiert werden. Dies kann nur von Personen durchgeführt werden, denen Vertrauen entgegengebracht wird. Aufgrund zum Teil gegensätzlicher Interessen zwischen Unternehmen und öffentlichen Dienstanbietern muß also die Verwaltung innerhalb des *Zuständigkeitsbereiches* des Unternehmens liegen. Deshalb können in unserem Beispiel Sicherheitsmechanismen zur Realisierung der genannten Schutzziele nicht innerhalb der öffentlichen Netze eingebracht werden.

3.1 Identifikation von Domains am Beispiel VPN

Domains werden zunächst möglichst groß gewählt und gegebenenfalls im Rahmen der näheren Untersuchung verfeinert. Einsparungs-Effekte können durch die übergreifende Realisierung von Sicherheitsanforderungen für einen möglichst großen Domain erreicht

werden. Beispielsweise kann das Verschlüsseln in einem Gateway die Verschlüsselung im angeschlossenen LAN ersetzen.

Für eine Partitionierung der Beispielkonfiguration seien zunächst die ihr zugrundeliegenden charakteristischen Eigenschaften gegeben:

Schützenswerte Daten, die innerhalb der LANs (Niederlassungen eines Unternehmens) verarbeitet werden, sind vor Ausspähung und unerkannter Veränderung zu schützen. Die Verfügbarkeit der schützenswerten Daten innerhalb der LANs und die Verfügbarkeit der Dienste der öffentlichen Netze zum Transport von Daten zwischen verschiedenen LANs soll nicht Gegenstand dieser Arbeit sein.

Die Zuständigkeiten für die LANs unterscheiden sich von denen der öffentlichen Netze. Dies impliziert eine erste Partitionierung der Beispielkonfiguration in die Domains LAN und öffentliches Netz (Bild 2a). Das Domain-Konzept sieht an dieser Stelle folgende Schritte zur Sicherung von schützenswerten Daten innerhalb der Gesamtkonfiguration vor:

(1) Sicherung der unsicheren Domains, in denen schützenswerte Daten verarbeitet werden. Eine dazu gegebenenfalls notwendige Verfeinerung des Modells wird solange fortgesetzt, bis sichere Domains vorliegen, die über Schnittstellen mit unsicheren Domains verbunden sind (z. B. sichere Rechner, unsichere Verbindung der Rechner). Dann wird zur Sicherung der unsicheren Domains nach (3) verfahren. An dieser Stelle nehmen wir nichtmanipulierte Software- und Hardware-Komponenten an, damit der Verfeinerungsprozeß nicht beliebig lange fortgesetzt werden muß.

(2) Gegenseitige Abgrenzung miteinander verbundener Domains zur Gewährleistung der Unabhängigkeit benachbarter Domains aus Sicherheitssicht. Diese Sicherung muß z. B. den Zugriff auf innerhalb eines Domains realisierte Sicherheitsfunktionalität oder schützenswerte Daten von angrenzenden Domains aus verhindern.

(3) Einfügen von Ende-zu-Ende-Sicherheitsmechanismen [2] in sichere Domains, die zu sichernde Daten verarbeiten, zur Sicherung dieser Daten bei ihrem Aufenthalt in benachbarten unsicheren Domains. Sicherheitsfunktionalität wird dabei immer in die Übergänge sicherer Domains zu angrenzenden, unsicheren Domains integriert, da in unsicheren Domains die Sicherheitsmechanismen nicht gegen Manipulation etc. geschützt wären. Die unsicheren Domains werden dadurch gesichert, daß in ihnen schützenswerte Daten nur in geschützter Form vorliegen. Diese geschützten Daten sind transportierbar, aber meist nicht verarbeitbar[1].

[1] verschlüsselte Daten können beispielsweise nicht interpretiert werden

Zur besseren Nachvollziehbarkeit der Vorgehensweise sind die im Folgenden angewendeten Schritte angegeben.

3.2 Verfeinerung des Domains LAN

Die Rollenverteilung innerhalb der LANs oder LAN-Verbunde impliziert meist differenzierte Rechte bezüglich des Zugriffs auf sensitive Daten. Als konkretes Beispiel wird ein LAN mit einer Datenbank angenommen. Damit zugriffsgeschützte Daten sicher beim autorisierten Anfrager ankommen, müssen diese auch auf ihrem Weg von der Datenbank zur anfragenden Teilnehmerstation geschützt werden. Innerhalb der LANs werden aufgrund differenzierter Angriffsmöglichkeiten die Domains Datenbank, Teilnehmerstation, Broadcast-Medium und Netzkopplung unterschieden (Schritt 1).

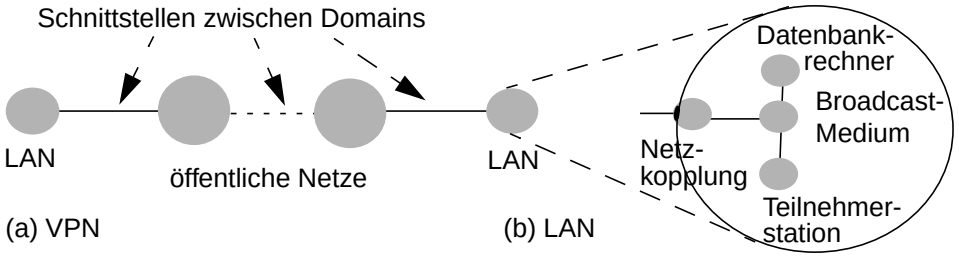

Bild 2: Domain-Modell der Beispielkonfiguration und Verfeinerung

Die *Datenbank* befinde sich in einem gesicherten Raum und sei auf einem dedizierten Rechner realisiert. In diesem Domain können Angriffe lediglich über die Anfrageschnittstelle erfolgen, indem ein Anfrager eine falsche Identität vorspiegelt, um unautorisiert auf schützenswerte Daten zugreifen zu können. Die *Teilnehmerstationen* müssen ebenfalls durch geeignete Verfahren gegen unautorisierten Zugang geschützt werden. Das *Broadcast-Medium* ist bezüglich der übertragenen Daten Abhörangriffen und verändernden Angriffen ausgesetzt [3]. Die *Netzkopplung* hat eine Sonderstellung, da sie die Schnittstelle des LANs zum öffentlichen Netz darstellt.

Das in Bild 2b verfeinerte Domain-Modell wird nun Schritt für Schritt gesichert. Im Bild sind Domains durch Knoten und Nachbarschaftsbeziehungen von Domains durch Kanten dargestellt.

3.3 Realisierung der Schutzziele innerhalb der LANs:

Der Zugriff auf die Stationen des LANs wird heute im allgemeinen durch ein Paßwortverfahren geschützt. Dabei weist der Teilnehmer zuerst seine Identität durch die Kenntnis eines Geheimnisses nach. Das System kontrolliert anschließend alle Aktionen des Teilnehmers anhand sogenannter Zugriffskontroll-Listen, in denen vermerkt ist, welcher Teilnehmer wie auf welche Daten und Dienste zugreifen darf (Schritt 2). Die Abgrenzung der verschiedenen Domains wird durch solche Zugangs- und Zugriffskontrollverfahren [4],[5] und

spezielle - auch physikalische - Zugriffssicherungen der Teilnehmerstationen gegen Manipulierbarkeit der Rechner-Software (z.B Booten von Diskette) und der Rechner-Hardware (z.B. Umprogrammieren der Netzkarte) erreicht.

Der Domain Broadcast-Medium innerhalb des LANs stellt einen unsicheren Domain dar. Da das Broadcast-Medium die schützenswerten Daten nicht verarbeiten, sondern nur transportieren muß, sollen Ende-zu-Ende-Sicherheitsmaßnahmen zum Einsatz kommen (Schritt 3). Diese sind in allen angeschlossenen Stationen zu integrieren. Für eine Möglichkeit zur Realisierung wird auf den „Secure Data Exchange“-Standard (SDE [6]) verwiesen, welcher die Eingliederung dieser Ende-zu-Ende-Sicherheitsfunktionalität oberhalb der Medienzugriffsschicht (Medium Access, MAC) des OSI-Referenzmodelles in die LAN-Stationen beschreibt. Dadurch ist der Domain Broadcast-Medium ebenfalls gesichert.

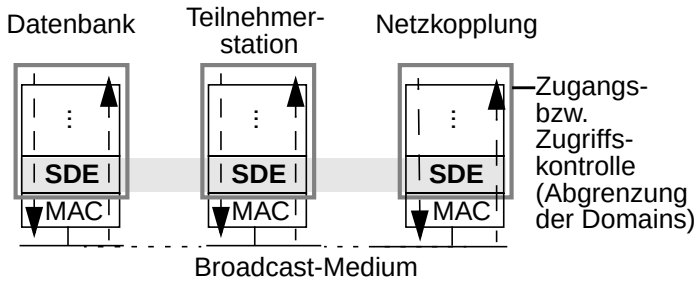

Bild 3: Sicherung des Domains LAN

In Bild 3 liegen schützenswerte Daten nur oberhalb der SDE-Schicht ungeschützt vor. Beim Durchgang durch die SDE-Schicht werden die Daten in Richtung Broadcast-Medium geschützt (mit einer Integritätsprüfsumme versehen und verschlüsselt). In Richtung Anwendung werden die geschützten Daten entschlüsselt und auf Integrität geprüft.

Falls innerhalb der LANs Zugriff auf DCE-Dienste (Distributed Computing Environment, [7]) besteht, so kann das LAN ergänzend durch DCE-Sicherheitsdienste geschützt werden. Innerhalb des DCE werden beispielsweise Paßwörter zur Identitätsprüfung verschlüsselt übertragen, was die Sicherheit heutiger Client-Server-Systeme erheblich verbessert.

Nachdem nun alle aus der Domain-Verfeinerung resultierenden Domains gesichert und gegeneinander abgegrenzt sind, können diese wieder zu einem Domain zusammengefaßt werden. Dieser gesicherte Domain LAN wird jetzt als *sicher* bezeichnet.

3.4 Realisierung der Schutzziele in den öffentlichen Netzen:

Schützenswerte Daten werden innerhalb der sicheren Domains LAN vor dem Überqueren der öffentlichen Netze mit kryptographischen Verfahren so geschützt, daß diese bezüglich der nun geschützten Objekte alle Sicherheitsanforderungen erfüllen und damit zu sicheren Domains für die geschützten Objekte werden (Schritt 3). Verschlüsselte Daten müssen beispielsweise

nicht vor Kenntnisnahme geschützt werden, um eine Ausspähung von Information zu verhindern. Diese Funktionalität wird in die Kommunikationsprotokolle des Netzüberganges zum öffentlichen Netz in die Netzkopplung integriert. Auf Transportebene kann dazu auf den ISO-Standard Transport Layer Security Protocol (TLSP [8]) zurückgegriffen werden. Die Verfügbarkeitsannahme für die öffentlichen Netze muß jedoch weiterhin gelten.

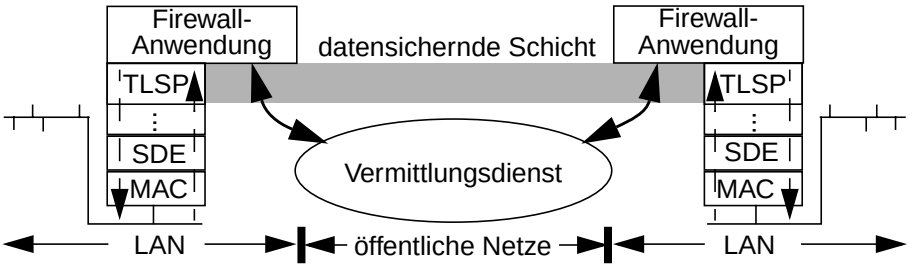

Bild 4: Ende-zu-Ende-Sicherung der F&E-Daten

Bild 4 zeigt auch die Plazierung eines sogenannten Firewalls [9], das den Übergang zwischen den sicheren Domains LAN und den unsicheren Domains öffentliche Netze kontrolliert (Schritt 2). Dadurch kann festgelegt werden, mit welchen Diensten von welchen Rechnern des öffentlichen Netzes aus auf das LAN zugegriffen werden darf und umgekehrt. Z. B. kann damit die Verwendung des sicheren Transportdienstes TLSP für die Übertragung von Daten zwischen LANs erzwungen werden. Auf diese Weise können auch unabsichtliche Sicherheitsverstöße wie das Versenden ungeschützter Daten über öffentliche Netze abgefangen werden. Zusätzlich dient das Firewall als Abgrenzung der LANs von den öffentlichen Netzen, so daß Sicherheitslücken innerhalb der LANs nicht von den öffentlichen Netzen aus ausgenutzt werden können.

4 Bewertung und Ausblick

Die vorgestellte Vorgehensweise zur Einordnung von Sicherheitsmechanismen zielt auf eine wirtschaftliche Lösung für Sicherheitsanforderungen ab. Gleichzeitig bleiben Sicherheitslücken lokal beschränkt und sind nicht über beliebige andere Netze nutzbar.

Für die Sicherheitsmechanismen selbst wurde dies gezeigt. Für die Organisation der Sicherheitsmechanismen, z.B. zur Realisierung von Ende-zu-Ende-Sicherheit, müssen jedoch auch Sicherheitsassoziationen zu ihrer Synchronisierung zwischen den Domains aufgebaut werden. Realisierungen solcher Sicherheitsassoziationen mit Hilfe der Signalisierung und die Erweiterung des Domain-Konzeptes auf den Schutz von Kommunikationsdaten befinden sich gerade in Arbeit.

5 Literatur

[1] J. Horgan: Thwarting the information thieves, IEEE Spectrum, Vol. 22, No. 7, July 1985, pp. 30-41

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

[3] C. Ruland: Datensicherheit in Lokalen Netzen - Teil I+II, DATACOM, Jahrgang 6, Heft12, 1989, pp. 94-99 und Jahrgang 7, Heft 1, 1990, pp. 100-107

[4] J. G. Steiner, C. Neuman, J. I. Schiller: Kerberos: An Authentication Service for Open Network Systems, Proceedings of the Winter Usenix Conference, 1988, pp. 191-202

[5] R. S. Sandhu, P. Samarati: Access Control: Principles and Practice, IEEE Communications Magazine, Vol. 32, No. 9, September 1994, pp. 40-48

[6] IEEE 802.10: IEEE Standards for Local and Metropolitan Area Networks: Interoperable LAN/MAN Security (SILS) - Secure Data Exchange (SDE), IEEE Standards Board, September 1992

[7] W. Rosenberry, D. Kenney: Understanding DCE, O‘Reilly&Associates, Inc., Sebastopol, 1993

[8] ISO/IEC 10736: Information Technology - Open Systems Interconnection - Transport Layer Security Protocol, January 1993

[9] S. M. Bellovin, W. R. Cheswick: Network Firewalls, IEEE Communications Magazine, Vol. 32, No. 9, September 1994, pp. 50-57

SONSTIGES:

Biographie:

Prof. Dr.-Ing P. J. Kühn studierte Elektrotechnik von 1962-1967 und promovierte 1972 zum Dr.-Ing. an der Universität Stuttgart. Nach Leitung einer Informatik-Forschungsgruppe und einer Industrietätigkeit bei den Bell Laboratorien in den USA nahm er 1978 einen Ruf für Nachrichtenvermittlung an die Universität Siegen und 1981 einen Ruf auf den Lehrstuhl für Nachrichtenvermittlung und Datenverarbeitung an die Universität Stuttgart an, der mit der Leitung des gleichnamigen Instituts verbunden ist. Seine Lehr- und Forschungsgebiete sind die Technische Informatik, Kommunikationsnetze und Nachrichtenverkehrstheorie. Seit 1991 leitet Prof. Kühn das Int. Advisory Council des Int. Teletraffic Congress (ITC). Er ist Mitglied der Heidelberger Akademie der Wissenschaften und der Leopoldina Halle und Professor Associé der Ecole Nationale Superieur de Telecommunications (ENST), Paris.

Dipl.-Inform. Reiner Sailer studierte von 1988-1994 Informatik an der Universität Karlsruhe. Seit 1994 ist er als wissenschaftlicher Angestellter am Institut für Nachrichtenvermittlung und Datenverarbeitung der Universität Stuttgart tätig. Er bearbeitet im Bereich der Kommunikationsnetze vor allem die Schwerpunktthemen Softwaretechnik, Protokolltechnik und Netzsicherheit.

Deutsche Zusammenfassung:

Zunächst wird ein Domain-Konzept vorgestellt, mit dessen Hilfe Mechanismen zur Erfüllung neuer Sicherheitsanforderungen in bestehende Kommunikationsinfrastruktur integriert werden können. Im Rahmen der Anwendung des Konzeptes auf eine beispielhafte Netzkonfiguration werden wesentliche Verfahren zur Sicherung von Kommunikationsnetzen beschrieben.

Englische Zusammenfassung:

A concept to enhance existing communications infrastructure by functionality to satisfy emerging security requirements is introduced. The proposed concept may serve as a guide for the integration of required security functionality. In the context of the concept’s application to an exemplary network configuration important available security mechanisms are described that can be applied to telecommunications.

Deutscher Titel:

Ein Domain-Konzept zur systematischen und wirtschaftlichen Integration von Sicherheit in Kommunikationsnetze

Englischer Titel:

Using a Domain Concept for Integrating Security into Communications Networks

Ansprechpartner-Adresse:

Dipl. -Inform. Reiner Sailer,
Universität Stuttgart,
Institut für Nachrichtenvermittlung und Datenverarbeitung (IND)
Seidenstraße 36
70174 Stuttgart
Telefon: 0711/121-2487
Telefax: 0711/121-2477
E-Mail: sailer@ind.uni-stuttgart.de