In: Brüggemann, H.-H.; Gerhardt, W. (Hrsg.): Proceedings der Fachtagung Verläßliche IT-Systeme - VIS '95. DuD-Fachberichte, Vieweg-Verlag, Braunschweig 1995, S. 163-180.

Guarded Authentic Local Area Network - GALAN -

Dirk Fox, Torsten Henn, Klaus Reichel*, Christoph Ruland

Institut für Nachrichtenübermittlung
Universität Siegen, 57068 Siegen
e-mail: fox@nue.et-inf.uni-siegen.de

Zusammenfassung

In lokalen Netzwerken stellen sich insbesondere wegen des *broadcast*-Charakters der existierenden LAN-Übertragungstechniken Fragen der Sicherheit der übertragenen Daten mit besonderer Dringlichkeit. Bei der Entwicklung von LAN-Protokollen und -Betriebssystemen beschränkten sich Sicherheitsvorkehrungen bisher jedoch meist auf Zugriffs- und Zugangskontrollmechanismen.

Das Sicherheitssystem GALAN ergänzt existierende heterogene lokale Netze um einen transparenten *link*-Schutz. Es ermöglicht die Kommunikation über geschützte und ungeschützte Verbindungen in einem Netzwerk sowie die Kopplung von geschützten und ungeschützten Teilnetzen über eine Sicherheits-Brükke. GALAN umfaßt die Sicherheitsdienste Vertraulichkeit, Datenintegrität, Zugangskontrolle und Authentisierung des Datenursprungs durch eine symmetrische *online*-Verschlüsselung aller Schicht-2-Nutzdaten (MAC-SDU). Die Sicherheitsbrücken vereinbaren für den Schutz von *backbone*-Kopplungen authentische *session keys*. In Verbindung mit einem authentischen Boot-Prozeß ermöglicht GALAN eine chipkartenbasierte Benutzerauthentisierung.

Für heterogene PC-LANs wurde ein GALAN-Prototyp, bestehend aus einen Endsystem-Dämonen und einer Sicherheitsbrücke implementiert. Das SDE-Protokoll im Endsystem setzt auf dem Protokollmultiplexer UPPS auf. Es schützt u.a. die verbreiteten LAN-Netzwerkprotokolle IPX, SPX, TCP/IP, UDP und DECNET in unterschiedlichen *client-server* und *peer-to-peer*-Betriebssystemen (wie Novell NetWare, Personal NetWare, LAN Manager, LAN Server, Banyan Vines, Windows for Workgroups und Windows NT) und für verschiedene Anwendungen (wie FTP, Telnet, WWW, E-Mail) unabhängig von Netztopologie und Übertragungsmedium (Token Ring, FDDI, Ethernet).

---

*Seit Jan. 1995 ISC Informatik Service & Consulting GmbH, Troisdorf

1 Einleitung

Isolierte Einzelplatzsysteme (PCs), die jeden Nutzer mit derselben Rechenleistung ausstatten, die er sich in Großrechnerumgebungen mit vielen Kollegen teilen mußte, werden zunehmend zu *lokalen Netzwerken* (LANs) zusammengeschlossen. Diese verbinden die Vorteile von Großrechneranlagen mit denen isolierter Einzelplatzsysteme: kontrollierbarer Zugriff auf gemeinsame Datenbestände, die Möglichkeit zentraler Wartung und Installation von Software bei gleichzeitig hoher Verfügbarkeit und großer Leistungsfähigkeit.

Neben die lokalen und zentralen Ressourcen treten in einer solchen informationstechnischen Umgebung die zu übertragenden Daten als wichtiges Schutzobjekt. Da die Übertragungstechniken in lokalen Netzwerken (Ethernet, Token Ring, FDDI) *broadcast*-Eigenschaft besitzen, durchlaufen sämtliche zu übertragenden Daten viele Kabelabschnitte des Netzwerkes. Außerdem werden im Unterschied zu einer Terminal-Verbindung nicht ausgewählte Ein-/Ausgabedaten, sondern Programme und Daten in Form kompletter Dateien übertragen. Ein Abhören des gesamten Datenverkehrs ist an fast jeder Stelle des Netzes möglich. Die Leistungsfähigkeit der Arbeitsstationen, die Verfügbarkeit von Netzwerk-Analysatoren, oft vorhandene freie Netzwerk-Anschlußdosen und die Möglichkeit, moderne Netzwerkadapter in der Betriebsart *promiscuous* (Empfang aller Datenpakete, unabhängig von der Empfängeradresse) zu betreiben, erleichtern einem Angreifer die Arbeit.

Daher ist neben einem Zugriffsschutz für zentrale Netzwerkressourcen, der in Netzwerkbetriebssystemen durch eine meist schwache und lediglich einseitige Benutzerauthentisierung (Login) verwirklicht wird, ein Schutz der Daten während der Übertragung erforderlich.

Bei der Entwicklung und Normung der LAN-Technologien und Protokolle in den achziger Jahren wurde Fragen der Datensicherheit zunächst eine untergeordnete Bedeutung beigemessen. Protokollimplementierungen für die unteren vier Schichten des ISO-OSI-Modells umfassen daher, von wenigen Speziallösungen abgesehen, bis heute keine Sicherheitsmechanismen. Erst Anfang der neunziger Jahre wurden Normenentwürfe vorgelegt, die eine Einbindung von Sicherheitsdiensten in Kommunikationsprotokolle vorsehen. Die Implementierung dieser Sicherheitsprotokolle und deren Integration in existierende Netzwerke gestaltet sich jedoch wegen der Heterogenität bestehender Netzwerke (viele Protokolle, zahlreiche Hersteller) schwierig.

Das Projekt *Guarded Authentic Local Area Network* (GALAN) verfolgt das Ziel, bestehende LANs in transparenter Form mit den Sicherheitsdiensten Vertraulichkeit, Datenintegrität, einer Authentisierung der Kommunikationspartner und des Datenursprungs sowie einem Zugangsschutz zu versehen.

2 Das Sicherheitssystem GALAN

Die Entwicklung eines in bestehende lokale Netze integrierbaren Sicherheitssystems für LANs muß einer Reihe von Randbedingungen genügen. Dazu zählen die Unterstützung existierender Übertragungsmedien, Kommunikationsprotokolle und Netzwerkbetriebssysteme sowie ein möglichst hoher Durchsatz und eine weitgehend transparente Realisierung. Diese Randbedingungen führten zu den folgenden Entwurfskriterien für das Sicherheitssystem GALAN:

- Einsetzbarkeit in Netzen unterschiedlicher Topologie, d.h. weitgehende Unabhängigkeit vom verwendeten Übertragungsmedium.
- Verwendbarkeit in heterogenen Kommunikationsumgebungen mit unterschiedlichen Netzwerk- und Transportprotokollen.
- Herstellerunabhängigkeit, d.h. Verwendung einer standardisierten oder möglichst verbreiteten Kommunikationsschnittstelle (API).
- Unabhängigkeit von Netzwerkbetriebssystem und (Kommunikations-) Anwendung.
- Möglichkeit zur weitgehend transparenten Integration in existierende Netzwerke.

Die Wahl einer geeigneten Protokollschicht zur Integration der genannten Sicherheitsdienste muß sich an diesen (praktischen) Randbedingungen orientieren. Nach ISO 7498-2 kommen grundsätzlich drei Schichten in Frage: die Transportschicht (4), die Netzwerkschicht (3) und die Sicherungsschicht (2) [ISO_89, MuRi_92, Rula_93].[1]

2.1 GALAN-Konzeption

Mit der Implementation eines Schicht-3- bzw. Schicht-4-Sicherheitsprotokolls wie beispielsweise das im Projekt *secure data network system* (SDNS) entwikkelte SP3 bzw. SP4, inzwischen als *network* bzw. *transport layer security protocol* genormt (NLSP/TLSP, ISO 10736/11577), läßt sich ein Ende-zu-Ende-Schutz mit den Sicherheitsdiensten Vertraulichkeit, Authentisierung der Partnerinstanz und des Datenursprungs, Datenintegrität und Zugangskontrolle realisieren [NeHe_89, ISO_89, ISO1_94, ISO2_94].

Bei einer solchen Lösung sind die Schicht-3-Nutzdaten auch in Brücken und Routern geschützt. Entscheidender Nachteil: Sämtliche vom Endsystem genutzten Schicht-3- bzw. Schicht-4-Protokollimplementierungen müssen um einen *security sublayer* ergänzt werden. Angesichts der Heterogenität existierender LANs und der Herstellervielzahl ist dies jedoch ein nicht praktikables Vorhaben. Zudem ist ein Ende-zu-Ende-Schutz auf die Protokollelemente der Trans-

[1] Streng genommen zählen auch die Anwendungsschicht (7) und (eingeschränkt) die Bitübertragungsschicht (1) dazu. Allerdings genügen beide nicht den Randbedingungen.

portschicht begrenzt; dadurch bleiben Anwendungen, die kein Netzwerk- oder Transportprotokoll verwenden, ebenso wie Protokollinformationen darunterliegender Schichten ungeschützt.

Aus diesen Gründen fiel die Entscheidung zugunsten eines Schutzes auf *link*-Ebene, wie in IEEE 802.10, *standard for interoperable LAN/MAN security*, empfohlen (SILS; [IEEE_93]). Das *secure data exchange sublayer* (SDE) wird dabei zwischen *medium access control sublayer* (MAC) und *logical link control* Teilschicht (LLC) in der Sicherungsschicht (2) angesiedelt.

Abweichend von den Vorschlägen der ISO 7498-2 (*security architecture*, [ISO_89]) sieht SILS neben Vertraulichkeit die Sicherheitsdienste Datenintegrität, Zugangskontrolle und Authentisierung des Datenursprungs vor. Das GALAN-SDE-Protokoll verzichtet jedoch auf die in SILS für die Erbringung dieser zusätzlichen Dienste vorgesehene (optionale) Ergänzung der *secure protocol data unit* (SPDU) um einen *integrity check value* (ICV) und einen *clear header*. Der Schutz beschränkt sich auf die Sicherheitsdienste Vertraulichkeit und Zugangskontrolle durch eine längeninvariante Verschlüsselung der *service data unit* (MAC-SDU, Bild 2-1). Die Sicherheitsdienste Datenintegrität und Authentisierung des Datenursprungs werden durch Verschlüsselung der Adressen, Folgenummern und Redundanzprüfwerte darüberliegender Protokolle indirekt erbracht.

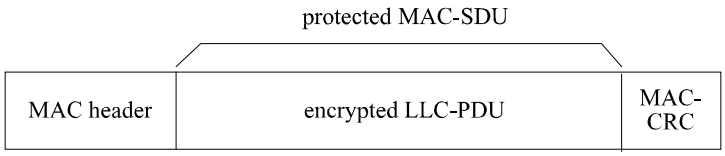

Bild 2-1: Verschlüsselung der MAC-SDU

Eine Überschreitung der maximalen Rahmenlänge kann so nicht auftreten; die SDE-Protokollschicht muß daher keine Mechanismen zur Fragmentierung und Reassemblierung vorsehen. Die Unterscheidung von geschützter und ungeschützter Übertragung trifft das SDE-Protokoll anhand der MAC-Adresse und interner Schlüsseltabellen.

Ein in Schicht 2 angesiedeltes SDE-Protokoll macht eine SDE-Protokollimplementierung in Routern zwischen zwei geschützt kommunizierenden GALAN-Endsystemen erforderlich. Häufig ist eine solche Erweiterung des Routers ohne weiteres nicht möglich; in den meisten Fällen sind spezielle Anpassungen notwendig.

Eine Alternative stellen transparente Sicherheitsbrücken dar, die vor und hinter dem Gateway für eine Ent- und ggf. erneute Verschlüsselung der MAC-SDUs sorgen. Die Integration einer solchen Sicherheitsbrücke in das Sicherheits-

system bietet einen weiteren großen Vorteil: Sie kann eine Wächter-Funktion für das dahinterliegende lokale Netz übernehmen. So lassen sich nicht nur Teilnetze mit und ohne *security associations* durch eine solche *guard bridge* trennen, sondern auch eine geschützte *backbone*-Kopplung von Teilnetzen realisieren (Bild 2-2).

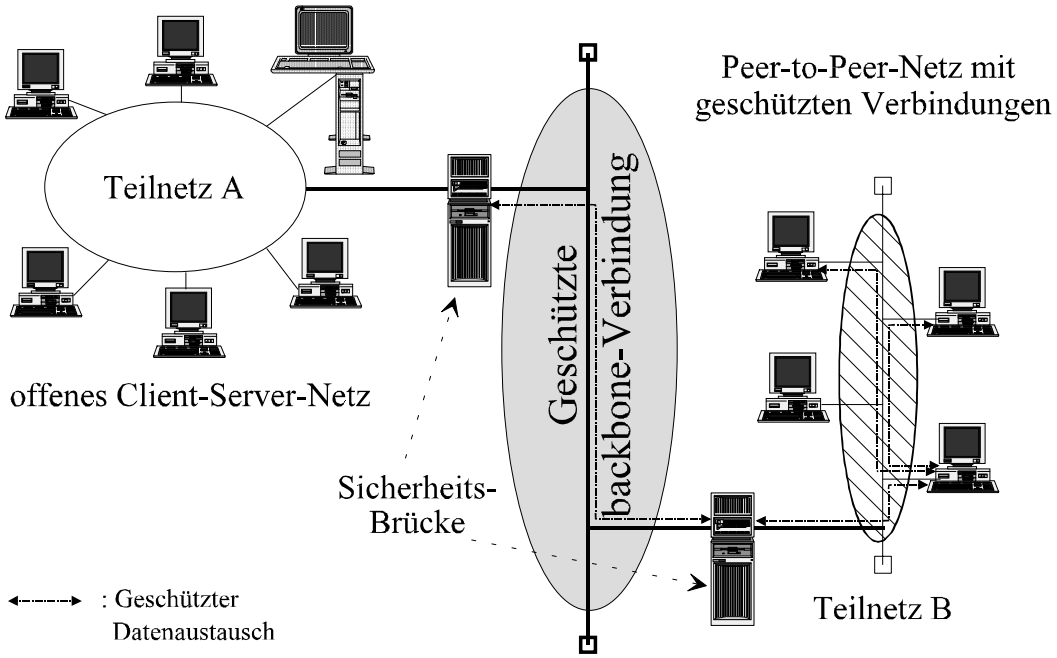

Bild 2-2: GALAN-Konfiguration (Beispiel)

Innerhalb eines Teilnetzes können wiederum geschützte und ungeschützte Verbindungen parallel betrieben werden. Die Sicherheitsbrücken können zusätzlich *firewall*-Funktionen für höhere Protokolle übernehmen [BaHS_93]; eine gegenseitige Authentisierung der Brücken sorgt dabei für einen wirkungsvollen Zugangsschutz.

2.2 GALAN-Sicherheitsdienste

Das GALAN-Sicherheitssystem realisiert einen *logical link*-Schutz nach SILS (IEEE 802.10). Es umfaßt die Sicherheitsdienste Vertraulichkeit, Zugangskontrolle und, in Verbindung mit höheren Protokollen, Datenintegrität und Authentisierung des Datenursprungs [ISO_89, IEEE_93].

2.2.1 Vertraulichkeit

Die Geheimhaltung der Nutzdaten bei der Übertragung ist ein wesentlicher Sicherheitsdienst des GALAN-Sicherheitssystems. Abhängig von der MAC-

Zieladresse werden alle Nutzdaten des MAC *sublayers* (LLC-PDU) mit einem symmetrischen Kryptoverfahren längeninvariant verschlüsselt. Dabei kommen wechselnde *session keys* zum Einsatz (siehe Abschnitt 2.3).[2]

2.2.2 Zugangskontrolle

Eine Zugangskontrolle erfolgt in verschiedener Hinsicht. Im Endsystem wird dieser Sicherheitsdienst implizit erbracht: Eine gesicherte Kommunikation setzt die Kenntnis eines symmetrischen *master* bzw. *session keys* voraus (siehe Abschnitt 2.3). Die Sicherheitsbrücke sorgt durch Filterung des Datenverkehrs dafür, daß nur Pakete mit zugelassenen MAC-Adressen die Brücke passieren. Ein Datenaustausch zwischen zwei Sicherheitsbrücken erfordert zudem die erfolgreiche Etablierung einer *security association*, d.h. die authentische Vereinbarung eines *session keys*.

2.2.3 Datenintegrität

Da die transparente Realisierung des *security sublayers* die Länge der Datenpakete unverändert läßt, erfolgt lediglich ein indirekter Integritätsschutz: durch die Verschlüsselung der Folgenummern bzw. Zeitstempel und Redundanzprüfwerte höherer Protokolle. Der Schutz ist damit allerdings – im Unterschied zu der in SILS vorgeschlagenen Anfügung eines *integrity check value* (ICV) – auf den Teil der verschlüsselten MAC-SDU beschränkt, der in die Berechnung des Prüfwertes eingeht.

2.2.4 Authentisierung des Datenursprungs

Auch dieser Sicherheitsdienst wird durch die Verschlüsselung der MAC-SDU indirekt erbracht, da der SDU kein *clear header* vorangestellt wird. Höhere LAN-Protokolle (IP, IPX) enthalten eindeutige Adressen, durch deren Verschlüsselung eine Authentisierung des Datenursprungs erfolgt.

2.3 GALAN-Schlüsselmanagement

Für die Erbringung der in Abschnitt 2.2 skizzierten Sicherheitsdienste sind geheime symmetrische Schlüssel erforderlich. Diese können Benutzer und Administratoren natürlich über einen separaten geheimen Kanal vereinbaren; ein solches Vorgehen ist jedoch meist aufwendig und erschwert einen regelmäßigen Schlüsselwechsel. GALAN sieht daher ein Schlüsselmanagement vor, das die

---

[2] Dieser Schlüssel für den sicheren Datenaustausch wird als *session key* bezeichnet, obwohl auf der Sicherungsschicht keine *sessions* im eigentlichen Sinne existieren.

Vereinbarung von *session keys* (Schlüssel mit begrenzter Gültigkeit) ermöglicht. Das Schlüsselmanagement zerfällt in zwei Einheiten: die Vergabe der *session keys* für die Kommunikation zwischen SDE-Dämonen in Endsystemen und den Schlüsselaustausch zwischen je zwei Sicherheitsbrücken.

2.3.1 Endsystem-Schlüssel

Da die Kommunikation zwischen zwei LAN-Endsystemen auf der Ebene des SDE-Protokolls verbindungslos erfolgt und keine *sessions*, d.h. Anfang und Ende einer Kommunikationsbeziehung bekannt sind, kann das authentische Schlüsselaustauschprotokoll mit der Partnerinstanz nicht beim Verbindungsaufbau durchgeführt werden. Aus diesem Grund sieht GALAN einen *online* verfügbaren Schlüsselserver vor, der (symmetrische) *session keys* für die gesicherte Kommunikation zwischen zwei Endsystemen generiert.

Bei der Installation des SDE-Dämonen in einem Endsystem meldet dieser sich beim Schlüsselserver an und führt ein Protokoll zur gegenseitigen Authentisierung durch. Dabei wird mit dem Schlüsselserver ein gemeinsamer symmetrischer *server key* vereinbart. Dieser Schlüssel behält seine Gültigkeit bis der SDE-Dämon sich explizit abmeldet oder (z.B. nach einem Systemabsturz) erneut authentisiert.

Will das Endsystem nun Daten gesichert an eine Partnerstation übertragen, fordert der SDE-Dämon einen symmetrischen *session key* beim Schlüsselserver an und trägt diesen in eine interne Tabelle ein. Empfängt der SDE-Dämon Daten von einem Endsystem, mit dem eine gesicherte Kommuniktion erfolgen soll, für das aber noch kein *session key* in seiner internen Tabelle eingetragen ist, läßt er sich den zugehörigen Schlüssel vom Schlüsselserver übermitteln.

Die Schlüssel zur Sicherung einer Kommunikationsbeziehung (Aufbau einer *security association*) zwischen zwei Endsystemen über dazwischenliegende Sicherheitsbrücken erfolgt für den Abschnitt vom Endsystem zur nächsten GALAN-Sicherheitsbrücke ähnlich: Die Brücke erhält den Schlüssel vom Schlüsselserver, wenn beide sich zuvor gegenseitig authentisiert haben und im Schlüsselserver das entfernte Endsystem als über diese Brücke erreichbar konfiguriert wurde.

In *peer-to-peer*-Umgebungen muß jeder SDE-Dämon neben dem *server key* alle *session keys* von geschützten Kommunikationsbeziehungen (*security associations*) mit einem Endsystem halten. Die auf diese Weise vereinbarten *session keys* verlieren ihre Gültigkeit nach Ablauf einer voreingestellten Frist; anschließend sind neue *session keys* beim Schlüsselserver anzufordern.

In *client-server*-Umgebungen kann das Schlüsselmanagement erheblich vereinfacht werden, indem der Schlüsselserver auf dem Netzwerkserver installiert

wird: Die vereinbarten *server keys* entsprechen dann gerade den *session keys* und genügen für den Schutz aller Kommunikationsbeziehungen, da auch der Datenaustausch zwischen den Clients über den Server abgewickelt wird.[3] Die SDE-Dämonen der Clients müssen lediglich den *server key* in ihrer Schlüsseltabelle halten. Eine Schlüsselvereinbarung findet mit jeder Anmeldung eines SDE-Dämonen beim Schlüsselserver und der anschließenden gegenseitigen Authentisierung statt.

2.3.2 Sicherheitsbrücken-Schlüssel

Zu Beginn jeder Kommunikationsbeziehung zwischen zwei GALAN-Sicherheitsbrücken wird eine *security association* etabliert. Dazu vereinbaren die Brücken authentisch einen gemeinsamen symmetrischen *session key*. Mit diesem werden alle über diese *backbone*-Verbindung zu übermittelnden Pakete verschlüsselt. Die Gültigkeit des im Rahmen dieses Protokolls ausgehandelten *session keys* kann zeitlich begrenzt werden; nach Ablauf der Gültigkeit wird ein neuer *session key* vereinbart.

Die authentische Schlüsselvereinbarung erfolgt mit einem zertifikatsbasierten asymmetrischen Schlüsselaustauschprotokoll, um eine vorausgehende Absprache symmetrischer *master keys* zu vermeiden.

2.4 Vertrauenswürdige Komponenten

Alle Komponenten des GALAN-Sicherheitssystems, die geheime Schlüssel oder andere sicherheitsrelevante Daten generieren oder aufbewahren, müssen vertrauenswürdig sein. Das gilt in besonderem Maße für die GALAN-Sicherheitsbrücken, die neben der Verschlüsselung auch Paketfilterungsfunktionen umfassen, und den Schlüsselserver, der alle symmetrischen *server keys* und sämtliche aktuellen *session keys* kennt. Diese Rechner sind gesondert (physisch und organisatorisch) zu schützen; die dort gehaltenen *session* und *master keys* sollten auch keinem Administrator zugänglich sein.

Auch das Endsystem muß vertrauenswürdig sein: Ein trojanisches Pferd kann sämtliche Sicherheitsmechanismen unterlaufen, indem es aktuelle *server* und *session keys* einem Angreifer zusendet. Will man einen aufwendigen (organisatorischen und physischen) Schutz der Arbeitsstationen umgehen, muß ein authentisches Booten lokal oder von einem physisch gesicherten Boot-Server erfolgen [OsSa_93, FoBö_94].

Durch eine Authentisierung des Benutzers gegenüber dem SDE-Dämonen (Paßwort, Chipkarte) kann die Authentisierung gegenüber dem Schlüsselserver

---

3 Dies setzt einen vertrauenswürdigen Netzwerkserver voraus.

auch benutzer- statt stationsbezogen erfolgen, wenn beispielsweise die Kommunikation bestimmter Benutzer über Teilnetzgrenzen hinaus durch die GALAN-Sicherheitsbrücke verhindert werden soll.

3 GALAN-Prototyp

Für PC-Netzwerke wurde ein GALAN-Prototyp entwickelt, bestehend aus einem SDE-Dämonen unter dem Betriebssystem DOS/Windows und einer Sicherheitsbrücke. Der Prototyp ermöglicht eine geschützte Kommunikation zwischen Arbeitsstationen, Servern und Sicherheitsbrücken unabhängig von Netzwerkbetriebssystem und Kommunikationsanwendung in Ethernet-, Token Ring- und FDDI-LANs. Der SDE-Dämon arbeitet mit festen, vorkonfigurierten Schlüsseln; eine Erweiterung um ein *online*-Schlüsselmanagement ist vorgesehen.

3.1 GALAN SDE-Dämon

Für Arbeitsstationen mit dem Betriebssystem DOS/Windows wurde ein SDE-Dämon implementiert, der auf einem verbreiteten Protokollmultiplexer aufsetzt und so die Nutzdaten aller auf diesem aufsetzenden Netzwerkprotokolle zugleich schützt. Neben geschützten sind auch Kommunikationsbeziehungen im Klartext zulässig. Sie werden anhand der MAC-Empfänger- bzw. -Senderadresse unterschieden und sind bei der Installation des SDE-Dämonen als Klartext-Beziehung zu konfigurieren.

3.1.1 Protokollmultiplexer

Die Unabhängigkeit sowohl von höheren Netzwerkprotokollen als auch von dem mediumspezifischen MAC-Rahmenformat kann durch die Verwendung eines verbreiteten und möglichst umfassenden Protokollmultiplexers, auch Multiprotokollstack genannt, erreicht werden. In PC-Netzen sind drei Multiprotokollstacks verbreitet (Bild 3-1, [Fish_90]):

- **NDIS** (*Network Driver Interface Specification*): Diese Spezifikation von Microsoft und 3Com, die inzwischen in einer erweiterten Version (ANDIS) auch von IBM (OS/2) unterstützt wird, stellt eine sehr umfangreiche Funktionsschnittstelle oberhalb des MAC *sublayers* für Kommunikationsanwendungen dar [Mi3C_90]. Es existieren unterschiedliche, zueinander inkompatible Versionsfamilien (NDIS 2.x und 3.x).

Die Schnittstelle liegt nicht sauber oberhalb einer Protokollschicht: Viele Funktionen sind mediumspezifisch, dadurch machte die Einführung neuer LAN-Übertragungstechniken (wie FDDI) eine Erweiterung der Spezifikation erforderlich [Stra_93]. NDIS-Treiber haben verglichen mit anderen Protokollmultiplexern einen hohen Speicherbedarf bei geringerem Datendurchsatz. NDIS-Treiber haben eine große Marktdurchdringung, da Microsoft-Betriebssysteme unmittelbar auf diesen aufsetzen.

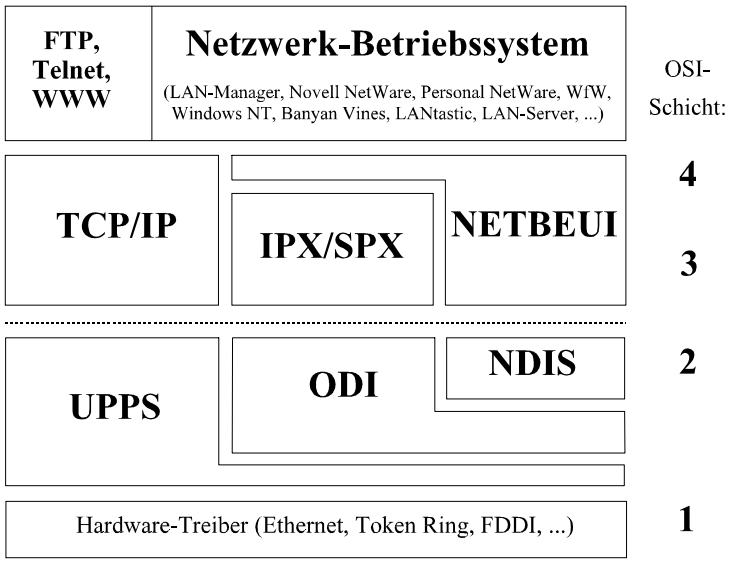

Bild 3-1: Einordnung und der wichtigsten (PC-) Protokollmultiplexer

- **ODI** (*Open Data-Link Interface*): Dieser Protokollmultiplexer ist eine Entwicklung der Firmen Novell und Apple Computer von 1989. Sie abstrahiert vollständig von den Eigenschaften des Übertragungsmediums und stellt über die LSL-Schnittstelle (*Link Support Layer*) oberhalb des MAC *sublayers* darüberliegenden Protokollen Sende-, Empfangs- und Diagnosefunktionen zur Verfügung [Nove_91].

  Die Schnittstelle ist sehr klar strukturiert; ODI-Treiber existieren für alle verbreiteten LAN-Adapterkarten. Von Novell sind ODI-Aufsätze verfügbar, die eine NDIS-Schnittstelle emulieren. Auf diese Weise können NDIS-basierte Protokollimplementierungen (wie beispielsweise NetBEUI) mit einem ODI-Multiplexer eingesetzt werden.
- **UPPS** (*Universal Portable Protocol Stack*) wurde von der Firma Schneider & Koch ursprünglich für die eigenentwickelten Netzwerkkarten konzipiert. Ähnlich ODI ist UPPS ein Multiprotokolltreiber, der vom darunterliegenden Medium (FDDI, Token Ring, Ethernet) vollständig abstrahiert und Kommunikationsfunktionen oberhalb der MAC-Teilschicht anbietet.

Es existieren auf UPPS aufsetzende Implementierungen der wichtigsten Protokolle sowie Emulatoren für ODI und NDIS. Der Multiprotokollstack unterstützt verschiedene Betriebsmodi wie z.B. die Nutzung desselben MAC-Rahmenformats durch mehrere Protokolle höherer Schichten (*chain mode*) und das Abfangen von Paketen vor deren Verteilung durch den Protokollmultiplexer (*hook mode*). Für Protokollimplementierungen existiert eine gut dokumentierte API [ScKo_93]. UPPS-Treiber zeichnen sich durch ein durchdachtes Pufferkonzept und sehr hohe Durchsatzraten aus.

Der GALAN-Prototyp verwendet UPPS, da diese Schnittstelle sich wegen der genannten Betriebsmodi besonders für die Implementierung des SDE-Dämonen eignet [Reic_94]. Die Schnittstellenemulatoren für ODI und NDIS erlauben zugleich den Schutz aller auf diesen Protokollmultiplexern aufsetzenden Protokolle. Von der Firma SysKonnect Inc. sind mit SK-Passport inzwischen auch UPPS-Treiber für viele Netzwerkadapter anderer Hersteller verfügbar.

3.1.2 Verschlüsselung

Als Verschlüsselungsverfahren finden zwei symmetrische Blockchiffren Verwendung: der 1977 in den USA standardisierte DES (*Data Encryption Standard*) und der noch junge, von der ETH Zürich in Zusammenarbeit mit der Schweizer Firma Ascom Tech entwickelte IDEA (*International Data Encryption Algorithm*) [LaMa_90, NBS_77].

Die Blockchiffre wird in der Betriebsart *Cipher Block Chaining* (CBC) eingesetzt [ISO_91]. Da CBC grundsätzlich einen Chiffretext erzeugt, dessen Länge ein ganzzahliges Vielfaches der Blocklänge der Chiffre ist (hier: 64 Bit bzw. 8 Byte), können Datenpakete so nicht längeninvariant verschlüsselt werden. Daher wurde das Padding des letzten Datenblocks durch eine Sonderbehandlung nach einem von Davies und Price vorgeschlagenen Verfahren ersetzt [DaPr_89, FuRi_94]. Der letzte Teilblock wird dabei mit den ersten Bits des zweifach verschlüsselten vorletzten Blocks XOR-verknüpft. Die Entschlüsselung erfolgt analog (Bild 3-2).

Der Initialisierungsvektor (IV) ist Teil des Schlüssels und wird mit diesem vereinbart und gewechselt.[4] Die Unterscheidung von zu schützenden und offenen Kommunikationsbeziehungen erfolgt anhand der MAC-Adresse der Partner-Instanz entsprechend den bei der Installation des SDE-Dämonen vorgenommenen Einstellungen (Konfigurationsdatei).

---

[4] Die Verwendung des zuletzt ent- bzw. verschlüsselten Blocks als IV für die Verschlüsselung des nächsten Pakets würde eine garantierte Paketreihenfolge erfordern.

$c_0 = E(k, m_0 \text{ XOR } IV)$	$m_0 = IV \text{ XOR } D(k, c_0)$
...	...
$c_i = E(k, m_i \text{ XOR } c_{i-1})$	$m_i = c_{i-1} \text{ XOR } D(k, c_i)$
...	...
$c_n = m_n \text{ XOR } j{:}E(k, c_{n-1})$	$m_n = c_n \text{ XOR } j{:}E(k, c_{n-1})$

Bild 3-2: CBC-Mode und Behandlung des letzten Blocks.
*(Dabei bedeuten: **E**:* encryption*; **D**:* decryption*; $\boldsymbol{m_i/c_i}$: i-ter Klar-/Schlüsseltextblock; **k**:* session key*; **IV**: Initialisierungsvektor; **j:x**: j-Anfang von x.)*

Eine besondere Behandlung erfordern *broadcast*- und *multicast*-Pakete. In der MAC-Empfängeradresse von *multicast*-Paketen ist das höchstwertige Bit gesetzt und weist die Adresse so als Gruppenadresse aus. Diese Adressen sind festgelegten Protokollen zugeordnet, die mehrere Empfänger haben. Eine typische *multicast*-Anwendung ist z.B. ein Netzwerkmanagementprotokoll. *Broadcast*-Pakete sind spezielle *multicast*-Pakete, die von allen Endsystemen eines Netzes empfangen und ausgewertet werden sollen. Sie haben die eindeutige Empfängeradresse `0xFF.FF.FF.FF.FF.FF`.

Eine verschlüsselte Übertragung von *broadcast*-Paketen erfordert die Konfiguration aller Stationen des Netzes mit einem gemeinsamen symmetrischen Schlüssel. Der Schutz von *multicast*-Paketen setzt die Verteilung des jeweiligen *multicast*-Schlüssels an alle Empfänger voraus.

Die in einem SDE-Dämonen zu verwaltende Schlüsseltabelle ist klein: In *client-server*-Netzen mit `n` Clients ist für eine geschützte Kommunikation lediglich je ein gemeinsamer Schlüssel für Server und Arbeitsstation erforderlich, da auch der Datenaustausch mit anderen Arbeitsstationen über den Server abgewickelt wird. Der Server muß maximal `n` Schlüssel halten. In *peer-to-peer*-Umgebungen wird je Arbeitsstationenpaar ein gemeinsamer Schlüssel benötigt; es müssen also bis zu `n-1` Schlüssel von einem SDE-Dämonen verwaltet werden.

Die authentische Installation des SDE-Dämonen (Schutz vor trojanischen Pferden) wird in *client-server*-Netzen (bisher nur unter Novell NetWare) durch einen authentischen *remote boot*-Prozeß sichergestellt [FoBö_94].

3.2 GALAN-Sicherheitsbrücke

Die Sicherheitsbrücke wurde als eine mit zwei Netzwerkadaptern ausgestattete Arbeitsstation realisiert. Sie besitzt volle Bridge-Funktionalität, d.h. kann Teilnetze mit unterschiedlichen Übertragungsmedien, MAC-Rahmenformaten und Topologien koppeln. Die Brücke umfaßt die Funktion zweier GALAN-Dämo-

nen, die ihr eine adreßabhängige geschützte Kommunikation mit Endsystemen und anderen GALAN-Sicherheitsbrücken erlaubt.

Die Netzwerkadapter werden im *promiscuous mode* betrieben, damit sie sämtliche Pakete unabhängig von der MAC-Empfängeradresse empfangen und auswerten können. Anhand interner, vorkonfigurierter Tabellen entscheiden sie in Abhängigkeit von der MAC-Sender- bzw. Empfängeradresse, ob ein Paket von einem Teilnetz in das andere zu übertragen und ggf. zuvor zu ver- oder entschlüsseln ist (Bild 3-3).

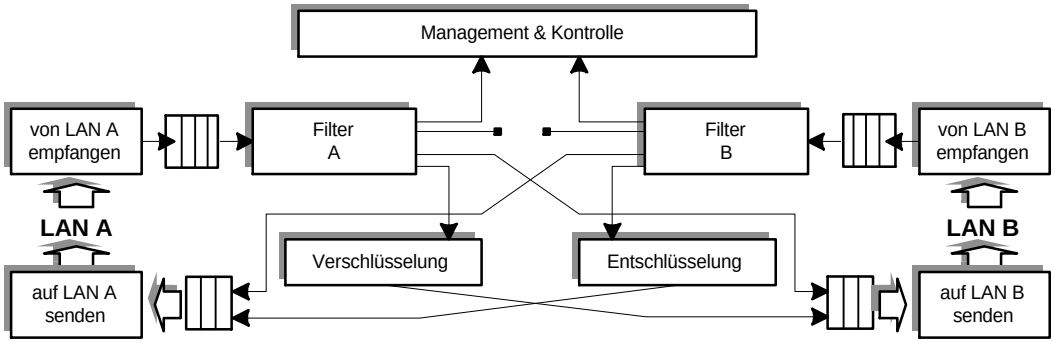

Bild 3-3: Arbeitsweise der GALAN-Sicherheitsbrücke (gesichertes backbone *Netz B; nach [RMSSF_93])*

Die Sicherheitsbrücke muß vollständig transparent realisiert werden, d.h. darf außer der Ver- bzw. Entschlüsselung von MAC-SDUs keine Veränderungen an den Paketen vornehmen, da anderenfalls eine korrekte Weiterleitung der Pakete nicht möglich wäre [Henn_94].

Damit auch die MAC-Absenderadresse im *header* des MAC-Paketes, die vom LAN-Adapter automatisch dort eingesetzt wird, erhalten bleibt, muß die korrekte Absenderadresse als (logische) Adapteradresse der Brücke eingestellt werden. Diese Adreßumstellung bewirkt allerdings Performanceeinbußen. Spürbar sind diese besonders in Token-Ring-Netzen, da dadurch jeweils eine Ab- und erneute Anmeldung im Ringmanagement erforderlich wird.[5] Um die Auswirkungen auf die Übertragungsgeschwindigkeit bei der Übertragung großer Datenmengen (*bursts*) zu begrenzen, wird vor der Adreßumstellung geprüft, ob bereits die erforderliche Adresse eingestellt ist.

Um mehrere Sicherheitsbrücken in einem Netz betreiben zu können, enthalten die Schlüsseltabellen neben der Zuordnung MAC-Adresse/Schlüssel auch Angaben darüber, in welchem Teilnetz sich ein Endsystem befindet (Adreßlisten) und von welchen Absendern bzw. an welche Empfänger Pakete weitergeleitet

---

5 Durch Nutzung des von IBM verwendeten *source routings* ließe sich dieses Problem umgehen. Dies ist jedoch eine proprietäre Lösung und verstößt gegen die IEEE-Empfehlung 802.5 [Kauf_94].

werden dürfen (Adreßfilterung). Die Adreßlisten können automatisch gelernt oder manuell vor- bzw. umkonfiguriert werden [Henn_94].

Die GALAN-Sicherheitsbrücke arbeitet mit zwei Ringpuffern, in die die von einem Adapter empfangenen Pakete nach Filterung und Ver- bzw. Entschlüsselung zur Weiterleitung über den jeweils anderen Adapter eingetragen werden. Ein Überlaufen der Ringpuffer führt zum Verlust von Datenpaketen und damit zu Performanceeinbrüchen. Die für einen reibungslosen Betrieb der Sicherheitsbrücke erforderliche Puffergröße wird bei der Installation konfiguriert. Sie hängt von mehreren Randbedingungen ab: der Geschwindigkeit des Datenbusses, der Netzwerkkarten, des Übertragungsmediums, dem Datenaufkommen, dem verwendeten Verschlüsselungsverfahren und dessen Realisierung.

Um den Durchsatz der Sicherheitsbrücke zu steigern, wurde in Anlehnung an [RMSSF_93] eine schnelle Adreßsuche durch Hashen implementiert. Als Hashwert dient dabei das letzte Byte der MAC-Adresse [Henn_94].

Die gegenseitige Authentisierung und Schlüsselvereinbarung zwischen den Sicherheitsbrücken erfolgt auf der Basis des *station to station*-Protokolls (STS, [DiOW_92]). Als digitales Signatursystem wird der standardisierte DSA (*Digital Signature Algorithm*) verwendet [Fox_93, NIST_94]). Die vereinbarten *session keys* verlieren ihre Gültigkeit nach einem voreingestellten Zeitraum. Das STS-Protokoll setzt auf dem SPX/IPX-Protokollstack auf.

3.3 Leistungsbetrachtungen

Der Speicherbedarf des GALAN-Dämonen liegt (ohne Verschlüsselungsmodul) bei etwa 17 KByte (speicherresident); hinzu kommen 4-9 KByte für die Verschlüsselungsoperationen. In der internen Adreß- und Schlüsseltabelle sind (inklusive Initialisierungsvektor) 22 Byte je Partnerinstanz abzulegen.

Der Durchsatz in einem GALAN-gesicherten Netzwerk hängt neben der allgemeinen Netzlast von dem verwendeten Kryptoverfahren (DES, IDEA; Hardware/Software) und vor allem von den Eigenschaften der eingesetzten PC-Hardware ab: Prozessorleistung, Geschwindigkeit des Datenbusses, verwendetes Übertragungsmedium, Wahl des LAN-Adapters der Sicherheitsbrücke (Busmaster, I/O, *memory mapped*). Diese Randbedingungen machen Messungen der Verweildauer von Daten in der GALAN-Sicherheitsbrücke wenig aussagekräftig. Bei sehr hoher Last kommt es in der Sicherheitsbrücke zu Paketverlusten (30-80%), insbesondere, wenn die Ringpuffer zu klein gewählt werden.

Die Bestimmung des Datendurchsatzes in einem Endsystem mit installiertem GALAN-Dämonen bei großer Last (*bursts*) gibt hingegen einen Anhaltspunkt für die (maximalen) Performanceeinbußen. Als Plattform wählten wir einen PC

mit ISA-Bus und einem mit 66 MHz getakteten 80486 DX/2 Mikroprozessor; gesendet wurden IPX-Pakete (Ethernet: 1000 Byte, Token Ring: 4500 Byte).

	Token Ring [MBit/s]	Ethernet [MBit/s]
Klartext	14,6 MBit/s	9,0 MBit/s
IDEA (Software)	3,7 MBit/s	3,5 MBit/s
DES (Hardware)	3,7 MBit/s	3,4 MBit/s

Tabelle 3-4: Durchsatzraten des GALAN-Dämonen [Reic_94]

Die Meßergebnisse in Tabelle 3-4 liefern für IDEA und DES ähnliche Resultate, die bei IDEA auf die hohe Prozessorbelastung des Verschlüsselungsalgorithmus, bei DES auf die CPU-intensive Ansteuerung der Hardware (I/O) und die Beschränkungen des Datenbusses (ISA) zurückzuführen sind. Der Durchsatz hängt daher allein von der Prozessorleistung und der Belastung durch die Netzwerkkarte ab, nicht aber von der Geschwindigkeit des Übertragungsmediums (Ethernet: 10 MBit/s, Token Ring: 16 MBit/s). Vergleichsmessungen auf Rechnern mit langsameren CPUs bestätigten dies.

Im praktischen Betrieb werden bessere Resultate erziehlt: Das Starten einer Anwendung vom Server über eine Sicherheitsbrücke verlangsamt sich um den Faktor 1,2-1,8.

4 Ausblick und Bewertung

Das Sicherheitssystem GALAN ermöglicht einen flexiblen Schutz der Kommunikation in heterogenen LANs auf *link*-Ebene. Durch die Verwendung des Multiprotokollstacks UPPS können unterschiedliche Netzwerkprotokolle zugleich geschützt werden. Der SDE-Dämon arbeitet dabei unabhängig von dem verwendeten Übertragungsmedium (Bild 4-1). Die vom ATM-Forum angekündigte Spezifikation der LAN-Emulationen wird voraussichtlich auch einen Betrieb des GALAN-Sicherheitssystems in ATM-basierten LANs erlauben [GaUn_94].

Der GALAN-Prototyp des SDE-Dämonen arbeitet mit festen, vorkonfigurierten Schlüsseln. Eine Version, die wechselnde *session keys* und den *online* verfügbaren Schlüsselserver nutzt, ist derzeit in Arbeit. Das Schlüsselaustauschprotokoll zwischen Endsystemen und Schlüsselserver erfolgt symmetrisch, angelehnt an das SECUVISOR-Protokoll [BöFo_93]. Die Authentisierung der Benutzer verwendet eine Paßworteingabe und Chipkarten.

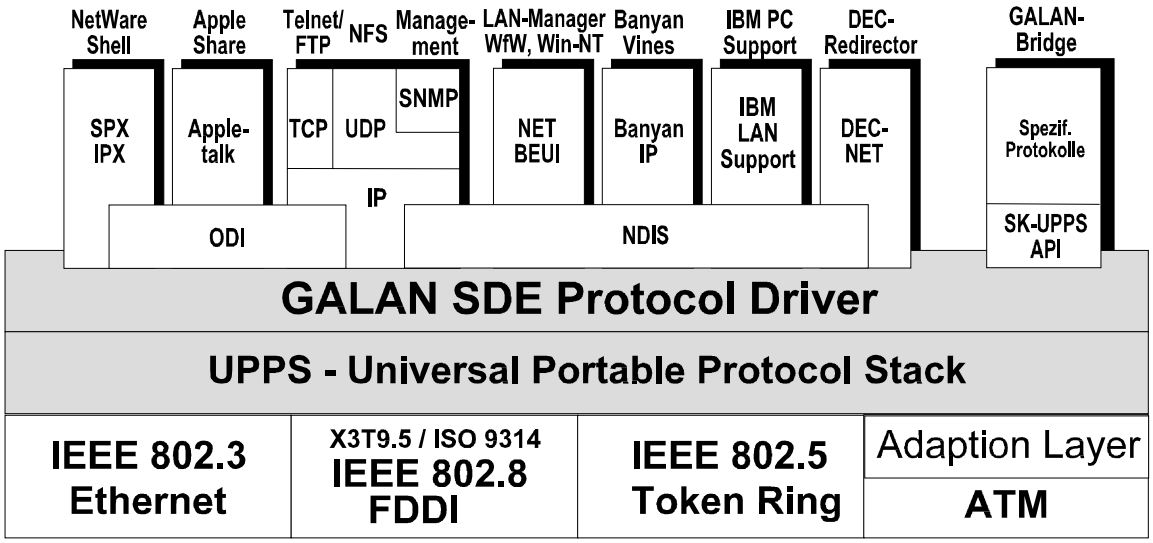

Bild 4-1: Sicherung heterogener Protokolle durch den GALAN-Dämonen.

Portierungen des GALAN-Clients auf andere PC-Betriebssysteme (Linux, OS/2, Windows 95/NT) werden die Beschränkung auf DOS-basierte Endsysteme aufheben. Eine Steigerung des Datendurchsatzes des GALAN-Dämonen und der Sicherheitsbrücke kann durch die folgenden Maßnahmen erreicht werden:

- Eine Implementierung des GALAN-Dämonen für spezielle Server-Betriebssysteme (z.B. Novell) würde die Sicherheitsbrücke zur Ver- und Entschlüsselung der Daten hinter bzw. vor dem Server überflüssig machen.
- Durch den Einsatz einer aktiven Verschlüsselungskarte (Busmaster) mit eigenem Prozessor, RAM und schnellem Systembus (MCA, EISA, PCI) ließe sich die Prozessorbelastung erheblich senken.
- Die Verwendung von Netzwerkadaptern mit einem Krypto-Chip *on board* würde den Bustransfer der Daten zu und von der Verschlüsselungskarte einsparen.

Dank

Klaus Reichel realisierte den GALAN-Dämonen des Prototyps für DOS/Windows [Reic_94]; Torsten Henn implementierte die GALAN-Sicherheitsbrücke [Henn_94]. Der Firma CEInfosys (Bodenheim) danken wir für die Leihstellung von DES-Hardware (WisoCrypt-Board). Unser Dank gilt auch den Gutachtern für die genaue Durchsicht des Beitrags und ihre hilfreiche Kritik.

Literatur

BaHS_93 Bauspieß, Fritz; Horster, Patrick; Stempel, Steffen: *Netzwerksicherheit durch selektiven Pakettransport*. In: Weck, G.; Horster, P. (Hrsg.): Verläßliche Informationssysteme, Proceedings der GI-Fachtagung VIS '93, DuD-Fachbeiträge 16, Vieweg, Braunschweig 1993, S. 395-415.

BöFo_93 Böttger, Manfred; Fox, Dirk: *SECUVISOR - ein technisches Schutzkonzept für Netzwerke*. In: Löw, H.-P.; Partosch, G. (Hrsg.): Verteilte Systeme - Organisation und Betrieb '93. Proceedings des 10. Fachgesprächs über Rechenzentren, Deutscher Universitäts-Verlag, Wiesbaden 1993, S. 248-262.

DaPr_89 Davies, Donald W.; Price, Wyn L.: *Security for Computer Networks*. 2. Auflage, John Wiley & Sons Ltd., Chichester 1989.

DiOW_92 Diffie, Whitfield; Oorschot, Paul C. van; Wiener, Michael J.: *Authentication and Authenticated Key Exchange*. Designs, Codes & Cryptography, Nr. 2, 1992, S. 107-125.

Fish_90 Fisher, Sharon: *Neue Treiber braucht das LAN: NDIS und ODLI*. c't magazin für computertechnik, Heft 11, 1991, S.350-353.

FoBö_94 Fox, Dirk; Böttger, Manfred: *SecuBoot - Authentisches Remote Boot für Client-Server-Netzwerke*. In: Bauknecht, K., Teufel, S. (Hrsg.): Sicherheit in Informationssystemen. Proceedings der Fachtagung SIS '94, vdf-Verlag, Zürich 1994, S. 161-173.

Fox_93 Fox, Dirk: *Der 'Digital Signature Standard': Aufwand, Implementierung und Sicherheit*. In: Weck, G.; Horster, P. (Hrsg.): Verläßliche Informationssysteme, Proceedings der GI-Fachtagung VIS '93, Vieweg, Braunschweig 1993, S. 333-352.

FuRi_94 Fumy, Walter; Rieß, Hans Peter: *Kryptographie*. Schriftenreihe Sicherheit in der Informationstechnik, Band 6. Oldenbourg Verlag, München, 2. Auflage 1994.

GaUn_94 Gamm, Christoph von; Ungerer, Bert: *Bausteine der Zukunft - ATM wird LAN und WAN vereinen*. c't magazin für computertechnik, 10/1994, S. 138-142.

Henn_94 Henn, Torsten: *Konzeption und Realisierung einer Security Bridge für heterogene LANs*. Diplomarbeit, Institut für Nachrichtenübermittlung, Universität Siegen, 12/1994.

IEEE_93 IEEE Std 802.10-1992: *Standards for Local and Metropolitan Area Networks: Interoperable LAN/MAN Security (SILS)*. Secure Data Exchange (SDE), 1993.

ISO_89 International Organisation for Standardization (ISO): *Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture*. International Standard ISO 7498-2 (E), Genf 1989.

ISO_91 International Organisation for Standardization (ISO): *Modes of Operations for an N-bit Block Cipher Algorithm*. International Standard ISO/IEC 10116, Genf 1991.

ISO1_94 International Organisation for Standardization (ISO): *Transport Layer Security Protocol*. International Standard ISO/IEC 10736, Genf 1994.

ISO2_94 International Organisation for Standardization (ISO): *Network Layer Security Protocol*. International Standard ISO/IEC 11577, Genf 1994.

Kauf_94 Kauffels, Franz-Joachim: *Lokale Netze*. 6. Auflage, Markt&Technik Verlag, München 1994.

LaMa_90 Lai, Xuejia; Massey, James L.: *A Proposal for a New Block Encryption Standard*. In: Damgård, I.B. (Hrsg.): Proceedings of Eurocrypt '90, LNCS 473, Springer, Berlin 1991, S. 389-404.

Mi3C_90 Microsoft, 3Com Corporation: *Network Driver Interface Specification (NDIS)*. Version 2.0.1, Mai 1990.

MuRi_92 Mund, Sibylle; Rieß, Hans Peter: *Kryptographische Protokolle für Sicherheit in Netzen*. Datenschutz und Datensicherung (DuD), 2/92, S. 72-80.

NBS_77 National Bureau of Standards (NBS): *Data Encryption Standard (DES)*. Federal Information Processing Standards Publication (FIPS-PUB) 46-1, US Department of Commerce, 1/1977.

NeHe_89 Nelson, Ruth; Heimann, John: *SDNS Architecture and End-to-End Encryption*. In: Brassard, G. (Hrsg.): Proceedings of Crypto '89. LNCS 435, Springer, Berlin 1990. S. 356-366.

NIST_94 National Institute of Standards and Technology (NIST): *Digital Signature Standard (DSS)*. Federal Information Processing Standards Publication 186 (FIPS-PUB), 19. Mai 1994.

Nove_91 Novell Inc.: *ODI Developers Guide for Network Protocols*, 1991.

OsSa_93 Osterlehner, Stefan; Sauerbrey, Jörg: *Authentisches Booten und Software-Integritätstest auf PC-Architekturen*. In: Weck, G.; Horster, P. (Hrsg.): Verläßliche Informationssysteme, Proceedings der GI-Fachtagung VIS '93, DuD-Fachbeiträge 16, Vieweg, Braunschweig 1993, S. 321-331.

Reic_94 Reichel, Klaus: *Entwicklung eines Sicherheitstreibers für LANs*. Diplomarbeit am Institut für Nachrichtenübermittlung, Universität Siegen, 9/1994.

RMSSF_93 Recacha, F.; Melús, J. L.; Simón, X.; Soriano, M.; Forné, J.: *Secure Data Transmission in Extended Ethernet Environments*. IEEE Journal on selected Areas in Communications, Vol. 11, No. 5, June 1993, S. 794-803.

Rula_93 Ruland, Christoph: *Informationssicherheit in Datennetzen*. DataCom-Verlag, Bergheim 1993.

ScKo_93 Schneider & Koch & Co. Datensysteme GmbH: *Universal Portable Protocol Stack (UPPS), Data Link Interface*. Version 2.8, Referenzhandbuch für Programmierer, September 1993.

Stra_93 Straßmann, Thomas: *Microsoft NDIS: Ein standardisierter Zugang zum Netz*. c't magazin für computertechnik, Heft 12, 1993, S. 260-264.