

*Technische Universität Darmstadt
Fachbereich Informatik
Kryptographie, Computeralgebra, Verteilte Systeme*

*Gutachter/Betreuer:
Prof. Dr. Johannes Buchmann
Dr. Thilo Zieschang*



Oliver Ferreau
(Oliver@Ferreau.de)

Sicherheit im ISDN

Diplomarbeit

April - Oktober 1997

Mein herzlicher Dank gilt allen, die diese Arbeit in der vorliegenden Form möglich gemacht und unterstützt haben. Dazu gehören in erster Linie Herr Professor Johannes Buchmann und Herr Dr. Thilo Zieschang als Gutachter und Betreuer im vergangenen halben Jahr.

Außerdem die Herren Macke, Hlavac und Schäfer von der Deutschen Telekom AG. Sie haben sich die Zeit genommen, mit mir technische Einzelheiten zu diskutieren.

Herr Sarbinowski (GMD) hat mir bereits in einem sehr frühen Stadium geholfen, viele wertvolle Kontakte herzustellen.

Aus mehreren Gesprächen mit Herrn Dipl.-Inf. Pordesch (GMD, früher provet) und aus seinen Büchern sind wertvolle Anregungen hervorgegangen.

Herrn Dipl.-Wirtsch.-Ing. Montag und den Damen aus der Telefonvermittlung der TUD danke ich für die praktischen Einblicke in die Telefonanlage der Hochschulregion Darmstadt.

Herr Dipl.-Ing. Blab beschäftigt sich bei der Firma Siemens mit der Sicherheit von Telefonanlagen und hat mir dankenswerterweise einige seiner Unterlagen zur Verfügung gestellt.

Herr Dipl.-Inf. Sailer arbeitet an der Universität Stuttgart an einem ähnlichen Themengebiet und hat mir freundlicherweise seine Unterlagen zur Verfügung gestellt.

Für die moralische und nicht zuletzt auch finanzielle Unterstützung danke ich außerdem meinen Eltern.

Darmstadt, im Oktober 1997

Oliver Ferreau

INHALT

1 EINLEITUNG	9
2 ISDN-ENDGERÄTE	11
2.1 Die ISDN-Verbindungstypen	11
2.1.1 Die Festverbindung	11
2.1.2 Die Wählverbindung	11
2.2 Die ISDN Anschlußtypen	12
2.2.1 Der ISDN-Basisanschluß	12
2.2.2 Der ISDN-Primärmultiplexanschluß	12
2.2.3 Zusammenfassung	13
2.3 ISDN-Dienste	13
2.4 Leistungs- und Komfortmerkmale	14
2.4.1 Verbindungsunabhängige Merkmale	14
2.4.2 Verbindungsabhängige Merkmale	14
2.5 ISDN-Endgeräte	15
2.5.1 ISDN-Telefone	15
2.5.2 ISDN-TK-Anlagen	15
2.5.3 Sonstige Endgeräte	16
2.6 Sicherheit bei ISDN-Dienstmerkmalen	16
2.6.1 Leistungs- und Komfortmerkmale in TK-Anlagen	16
2.6.2 Abhören von Räumen	17
2.6.3 Abhören von Telefongesprächen	17
2.7 Angreifbarkeit von TK-Anlagen	18
2.7.1 Angriffe durch Außentäter	18
2.7.1.1 Fernwartungszugang	20
2.7.1.2 Angriffe über den D-Kanal	20
2.7.2 Angriffe durch Innentäter	21
2.7.3 Kommunikationsprofile	21
2.7.4 Fazit	21
2.8 ISDN-vernetzte Rechner	22
2.9 Zusammenfassung	23
3 DER D-KANAL UND DIE VERMITTLUNGSSTELLEN	25
3.1 Einleitung	25
3.2 Der ISDN-D-Kanal	25
3.3 Aufgaben des D-Kanals	25
3.4 Aufbau des D-Kanals	26
3.4.1 Schicht 1 - physikalische Schicht	26
3.4.2 Schicht 2 - Sicherheitsschicht	26
3.4.3 Schicht 3 - Vermittlungsschicht	26

3.4.4 Bitfehlerrate	27
3.5 Reichweite des D-Kanals	27
3.5.1 Punkt-zu-Punkt-Verbindung	27
3.5.2 Punkt-zu-Mehrpunkt-Verbindung	27
3.5.3 Zwischen der Vermittlungsstelle und dem Endgerät	27
3.5.4 Zwischen der TK-Anlage und dem Endgerät	28
3.5.5 Auf einem 16 (D ₁₆) oder 64 kBit-D-Kanal (D ₆₄)	28
3.6 Ablauf eines Telefonats aus Sicht des D-Kanals	29
3.7 Angriffe auf den D-Kanal	29
3.7.1 Abhören	30
3.7.2 Abhören des Busses	31
3.8 Vermittlungsstellen	32
3.8.1 Die Vermittlungssoftware	32
3.8.2 Das Testzentrum der Telekom in Nürnberg	33
3.9 Schwachstellen in /Angriffe auf Vermittlungsstellen	33
3.9.1 Eindringen in die Vermittlungsstelle	33
3.9.2 Gefahrenpotential von Centrex-Teilnehmern	35
3.9.3 Umkonfigurieren von Anschlüssen	36
3.9.4 Abhören von Gesprächen/Räumen	36
3.9.5 Kostenloses Telefonieren	37
3.9.5.1 Blueboxing	37
3.9.5.2 Über die Telefonanlagen von Firmen	37
3.9.5.3 Abschalten der Gebührenerfassung	37
3.9.6 Denial of Service durch Prüfschleifen	38
3.9.7 Kostenlose Datenübertragung im D-Kanal	38
3.9.8 Das Geschäft mit den 0190-Nummern	39
3.9.9 Manipulation anderer Vermittlungsstellen	40
4 DAS ZEICHENGABESYSTEM 7	41
4.1 Einleitung	41
4.2 Zeichengabesysteme	41
4.2.1 Im-Band-Signalisierung	41
4.2.2 Das Problem des Blueboxing	42
4.2.3 Außer-Band-Signalisierung	42
4.3 Der Aufbau des CCITT Zeichengabesystems 7	43
4.3.1 Der message-transfer-part MTP	43
4.3.2 Der ISDN-user-part ISUP	43
4.3.3 Der signalling-connection-control-part SCCP	44
4.3.4 Der transaction-capability-application-part TCAP	44
4.3.5 Der operations-maintenance-and-administration-part OMAP	45
4.4 Zeichengabe-7-Netzwerke	45
4.4.1 Aufbau und Bestandteile	45
4.4.2 Kapazität des Zeichengabenetzes	46
4.4.3 Routing im ZGS-7	46
4.4.4 Netzübergänge	47
4.4.5 Das Telekom-Netz	47
4.4.6 Das nationale Netz	47
4.4.7 Das internationale Netz	48
4.4.8 Interworking	49

Sicherheit im ISDN	5
4.5 Ablauf eines Telefonats aus Sicht des Zeichengabesystems	50
4.5.1 Zwischen dem Anrufer und seiner Ortsvermittlungsstelle	50
4.5.2 Zwischen der Ursprungs- und der Transitvermittlungsstelle	50
4.5.3 Zwischen der Transit- und der Zielvermittlungsstelle	51
4.5.4 Zwischen der Zielvermittlungsstelle und dem Angerufenen	51
4.6 Sicherheit im Zeichengabesystem 7	51
4.6.1 Transitnetze und Paketfilter in den Netzübergängen	51
4.6.2 Umleitung bei Ausfall eines Knotens	52
4.6.3 Lastabwehr	52
4.6.4 Das Überwachungssystem AcceSS7	52
4.7 Angriffe auf das Zeichengabesystem 7	53
4.7.1 Künstliche Überlast	53
4.7.2 Mißbrauch der Zustandskennungen	54
4.7.3 Angriffe aus anderen Zeichengabesystemen	54
4.7.4 Angriffe auf Vermittlungsstellen	55
4.7.5 Überlisten der Netzübergänge	55
5 BEDEUTUNG DER SICHERHEITSLÜCKEN UND RISIKEN	57
5.1 Bewertungskriterien	57
5.1.1 Anzahl der Betroffenen	57
5.1.2 Art und Umfang des Schadens	57
5.1.3 Dauer der Schädigung	58
5.1.4 Verantwortungsbereich	58
5.2 Bedeutung für den Netzbetreiber	59
5.2.1 Einleitung	59
5.2.2 User-user-Mißbrauch	59
5.2.3 0190-Gebührenbetrug	59
5.2.4 Netzausfall durch Sabotage	60
5.2.5 Aufkleben auf D-Kanal oder das ZGS-7	61
5.2.6 Überlast im ZGS-7-Netz	62
5.2.7 SEPT-Mißbrauch	63
5.2.8 Vermittlungsstellensoftware	63
5.3 Bedeutung für den Kunden	64
5.3.1 Abhören von Gesprächen	64
5.3.2 Abhören gespeicherter Nachrichten	65
5.3.3 Abhören von Räumen	65
5.3.4 Angriffe über den D-Kanal	66
5.3.5 Angriffe auf Rechner/Rechnernetze	66
5.3.6 Telefonieren auf fremde Rechnung	66
5.4 Datenschutzrechtliche Aspekte	67
5.4.1 In den Vermittlungsstellen	67
5.4.2 In ISDN-Anlagen	68
6 VERSCHLÜSSELUNG IM ISDN	69
6.1 Einleitung	69
6.2 Verschlüsselungsverfahren	69
6.2.1 Symmetrische und asymmetrische Kryptographie	69
6.2.2 Blockchiffren	71
6.2.3 Stromchiffren	71

6.3 Verschlüsselungsmöglichkeiten im ISDN	72
6.3.1 Abschnittsweise Verschlüsselung	72
6.3.2 Ende-zu-Ende-Verschlüsselung	72
6.3.3 Verschlüsselung der B-Kanäle	72
6.3.4 Verschlüsselung des D-Kanals	73
6.3.5 Verschlüsselung der ZGS-7-Kanäle	74
6.3.6 Verschlüsselung innerhalb der ISDN-TK-Anlagen	74
6.4 Wer will überhaupt verschlüsseln?	75
6.5 Besondere Anforderungen des ISDN an die Verschlüsselung	76
6.5.1 Sehr große Teilnehmerzahl	76
6.5.2 Verzögerungen	76
6.5.3 Schlüssellänge	77
6.5.4 Konferenzschaltungen	77
6.5.5 Länge des Schlüsseltextes	77
6.5.6 Gültigkeitsdauer	78
6.6 Eignung/Anpassung bekannter Verfahren	78
6.6.1 Abschnittsweise oder Ende-zu-Ende-Verschlüsselung?	78
6.6.2 Symmetrisches oder asymmetrisches Verfahren?	78
6.6.3 Block- oder Stromchiffre?	79
7 AUTHENTIFIZIERUNG IM ISDN	81
7.1 Einleitung	81
7.2 Bekannte Authentifizierungsverfahren	81
7.2.1 Secret-key-Authentifizierung	81
7.2.2 Public-key-Authentifizierung	82
7.2.3 Authentifizierung mit Einmalpaßwörtern	82
7.2.4 Einseitige und gegenseitige Authentifizierung	83
7.3 Authentifizierungsmöglichkeiten im ISDN	83
7.3.1 Authentifizierung innerhalb einer TK-Anlage	83
7.3.2 Authentifizierung im D-Kanal	84
7.3.3 Authentifizierung im ZGS-7	84
7.3.4 Ende-zu-Ende-Authentifizierung	85
7.4 besondere Anforderungen des ISDN an die Authentifizierung	86
7.4.1 Allgemeine Anforderungen	86
7.4.2 Bei Ende-zu-Ende-Authentifizierung	86
7.4.3 Bei Authentifizierung zwischen Benutzer und Netz	87
7.5 Eignung/Anpassung bekannter Verfahren	87
8 FIREWALLS	89
8.1 Einleitung	89
8.2 Firewalls im Internet	89
8.2.1 Funktionsweise	89
8.2.2 Betriebsmodi	91
8.2.3 Produkte	91
8.2.4 Problem IP-Spoofing	91
8.3 Firewalls im ISDN	92

Sicherheit im ISDN	7
8.4 Firewalls in ISDN-TK-Anlagen	92
8.4.1 Firewall im D-Kanal	92
8.4.2 Absichern des Fernwartungszugangs	92
8.5 Firewalls in Vermittlungsstellen	93
8.5.1 Schutz vor Angriffen über Teilnehmerleitungen	93
8.5.2 Schutz vor Angriffen über das Zeichengabenetz	93
8.6 Firewalls im Zeichengabenetz	93
8.6.1 In den Zeichengabepunkten	93
8.6.2 An den Netzübergängen	94
ANHANG: LITERATURVERZEICHNIS	95

1 Einleitung

ISDN - das diensteintegrierende digitale Netz für die Daten- und Telekommunikation ist seit seiner Einführung Ende der achtziger Jahre auf dem Vormarsch. 1993 wurde es europaweit genormt. Seitdem wird es als Euro-ISDN bezeichnet.

Heute ziert ein ISDN-Telefon nahezu jedes Büro und auch der Einzug in die Privathaushalte ist nicht mehr aufzuhalten. Zur Zeit bestehen wegen der großen Nachfrage im Netz der Deutschen Telekom Engpässe, so daß vielerorts keine neuen ISDN-Anschlüsse zu bekommen sind.

Die Telekommunikation insgesamt gewinnt in unserer vernetzten Gesellschaft zunehmend an Bedeutung. Doch wie steht es um die Sicherheit?

Die Sicherheit der Computer und Computernetze wie dem Internet ist in aller Munde - aber Sicherheit in einem Telefonnetz?

Dabei ist das ISDN mehr als ein Telefonnetz: Es integriert alle Kommunikationsdienste, für die es bisher verschiedene eigene Netze gab. Darüber hinaus stellt es Leistungsmerkmale zur Verfügung, die es in Deutschland bisher nicht gab. Als digitales Kommunikationsnetz hat es mehr Gemeinsamkeiten mit den Computernetzen als bisherige Netze für einzelne Dienste. Die einzelnen Vermittlungsstellen im ISDN sind im Grunde spezielle Computer, die durch Software gesteuert werden. Auch die ISDN-Anlagen und -Telefone sind softwaregesteuert. Durch einfachen Austausch der Software können neue Dienst- und Leistungsmerkmale genutzt werden.

Aber mit den neuen Möglichkeiten sind auch neue Risiken verbunden. Durch eine Reihe zusätzlicher Merkmale in Telefonanlagen und Tischgeräten lassen sich unter Umständen Räume oder Gespräche abhören und Kommunikationsprofile einzelner Mitarbeiter oder ganzer Firmen erstellen.

Auf höheren Ebenen lassen sich Vermittlungsstellen oder sogar ganze Telefonnetze manipulieren.

Natürlich wissen die Hersteller und Betreiber der ISDN-Hardware, wie wichtig die Sicherheit ihrer Geräte und Netze ist. Man konnte sich bei der internationalen Normierung aber nicht auf gemeinsame Verschlüsselungs- und Authentifizierungsmethoden einigen. Deshalb sieht der Euro-ISDN-Standard solche Sicherheitsmerkmale nicht vor.

Erst der entstehende Wettbewerb durch die Zulassung verschiedener privater Festnetzbetreiber wird auch die Sicherheit zu einem wichtigen Verkaufsargument werden lassen. Vorerst sind die Betreiber und Nutzer von Endgeräten darauf angewiesen, sich selbst um die Sicherheit im Bereich Telekommunikation zu kümmern oder Spezialfirmen zu beauftragen, eine Sicherheitsanalyse anzufertigen.

Die vorliegende Arbeit befaßt sich in zwei Teilen mit der Sicherheit im ISDN:

Der erste Teil umfaßt die Kapitel zwei bis fünf und beschäftigt sich mit den Schwachstellen und Sicherheitslücken in den verschiedenen Ebenen des ISDN sowie deren Bedeutung für die jeweils Betroffenen.

An diese Einleitung schließt sich im zweiten Kapitel eine Untersuchung der Schwachstellen in ISDN-Endgeräten an. Dazu gehören neben den ISDN-Telefonen und anderen

speziellen Endgeräten für einzelne Dienste auch die ISDN-Karten für Computer und die ISDN-TK-Anlagen.

Im dritten Kapitel werden die Schwachstellen der Übertragung zwischen dem Benutzer und der Vermittlungsstelle sowie in den Vermittlungsstellen betrachtet.

Das vierte Kapitel befaßt sich mit der Sicherheit im Telekommunikationsnetz oberhalb der Vermittlungsstellen. Dazu gehören die Kommunikation der Vermittlungsstellen untereinander und der Austausch von Informationen über die Grenzen eines Netzes hinweg.

Das fünfte Kapitel faßt die aufgezeigten Schwachstellen in den ersten vier Kapiteln zusammen und bewertet sie unter verschiedenen Gesichtspunkten.

Der zweite Teil umfaßt die Kapitel sechs bis acht. Hier werden Lösungsansätze für die aufgezeigten Sicherheitslücken vorgestellt.

Im sechsten Kapitel geht es um Verschlüsselung im ISDN. Die verschiedenen Einsatzgebiete der Verschlüsselung werden untersucht und ihre besonderen Anforderungen dargestellt. Bekannte Verschlüsselungsverfahren werden auf ihre Eignung für den Einsatz im ISDN geprüft.

Im siebten Kapitel schließt sich die Authentifizierung an. Die Möglichkeiten zur Authentifizierung im ISDN werden untersucht. Die besonderen Anforderungen des ISDN an die Authentifizierung werden dargestellt und auch hier werden bekannte Verfahren auf ihre Eignung untersucht.

Das achte Kapitel ist dem Einsatz von Firewalls gewidmet. Es wird untersucht, ob und an welchen Stellen die aus dem Internet bekannten Filtermechanismen auch im ISDN eingesetzt werden können, um die Sicherheit zu erhöhen.

Die vorliegende Studie kann und will keine produktspezifischen Sicherheitslücken aufzeigen. Der Endgerätemarkt für das ISDN ist wegen der großen Nachfrage im Umbruch wie nie zuvor. Untersuchungen einzelner Produkte sind deshalb immer nur eine Momentaufnahme. Außerdem gibt es zu viele Faktoren, die in die Sicherheit mit hineinspielen. Ich habe mich deshalb auf generelle Sicherheitsprobleme beschränkt, die jeweils zumindest für einen großen Teil der ISDN-Benutzer relevant sind.

Diese Studie soll in Zukunft weiterentwickelt werden. Für Anregungen, Kritik und Verbesserungsvorschläge bin ich deshalb jederzeit sehr dankbar. Sie erreichen mich am besten per e-mail: Oliver@Ferreau.de

2 ISDN-Endgeräte

Meine Untersuchungen zum Thema Sicherheit im ISDN beginnen bei den Endgeräten, also auf der Benutzerseite. Dabei umfaßt der Begriff Endgeräte alles, was auf Benutzerseite angeschlossen werden kann. Dazu gehören unter anderem Telefone, Telefaxgeräte, Telekommunikationsanlagen und ISDN-PC-Karten.

Alles, was ein typischer Benutzer vom ISDN kennt und sieht, sind sein Telefon, ggf. seine Telefonanlage und der Anschluß. Diese werden deshalb zunächst systematisch dargestellt. Anschließend werden die Schwachstellen in puncto Sicherheit beschrieben.

Im Euro-ISDN gibt es eine ganze Palette verschiedener ISDN-Leitungs- und Anschlußtypen. Zunächst wird unterschieden zwischen digitalen Fest- und Wählverbindungen:

2.1 Die ISDN-Verbindungstypen

2.1.1 Die Festverbindung

Eine Festverbindung ist eine dauerhaft fest geschaltete Verbindung zwischen zwei Punkten. Sie ist in verschiedenen Übertragungsbandbreiten zwischen 64kbit/sec und 155Mbit/sec verfügbar. Festverbindungen werden hauptsächlich für den Aufbau von wide-area-Rechnernetzen (WAN) und die Übertragung von Rundfunk- und Fernsehprogrammen von den Studios zu den Sendeeinrichtungen.

2.1.2 Die Wählverbindung

Ein Anschluß für eine Wählverbindung umfaßt die Möglichkeit, sich seinen Kommunikationspartner vor jeder Verbindung auszusuchen. Ein solcher Anschluß wird für die kurzzeitige Übertragung von z.B. Sprache, Bewegtbildern, Telefaxen, Telex und Daten genutzt. Er ist in einer Bandbreite von je 64kbit/sec verfügbar. Durch Kanalbündelung sind auch hier höhere Bandbreiten möglich, was aber nur in ganz bestimmten Anwendungsfällen Sinn macht, z.B. bei Videokonferenzen.

Im Rahmen dieser Arbeit wird nur die Wählverbindung betrachtet. Bei Festverbindungen, die zum Aufbau von Computernetzwerken verwendet werden, kann die benötigte Sicherheit in den Computer-Netzwerk-Protokollen implementiert werden und bei Rundfunk- und Fernsehübertragungen, die im selben Moment ohnehin öffentlich ausgestrahlt werden, spielen nur die Ausfallsicherheit und die Authentizität eine Rolle. Sie abzuhören macht keinen Sinn.

Außerdem sind Festverbindungen vollständig vom Wählleitungsnetz abgekoppelt, so daß auch keine Angriffe hierüber erfolgen können.

Ein Anschluß für Wählverbindungen umfaßt immer eine gewisse Anzahl von Nutzkanälen, die sogenannten B-Kanäle, und einen zusätzlichen Kanal zu deren Steuerung, den D-Kanal. Sie werden später näher beschrieben und untersucht.¹

¹ Kapitel 3 befaßt sich mit der Sicherheit des D-Kanals.

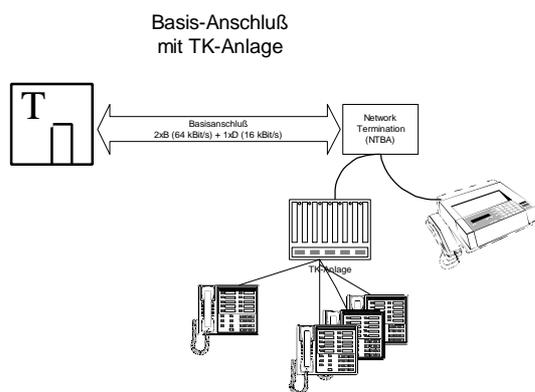
2.2 Die ISDN Anschlußtypen²

2.2.1 Der ISDN-Basisanschluß

Der sogenannte Basisanschluß stellt dem Benutzer zwei B-Kanäle mit einer Bandbreite von je 64 kBit/sec zur Verfügung, die von einem 16kbit/sec-D-Kanal gesteuert werden.

Man unterscheidet beim Basisanschluß eine Anlagen- und eine Mehrgerätevariante. Am Anlagenanschluß³ muß zwingend eine Telefonanlage angeschaltet werden, die wiederum die angeschlossenen Telefone und sonstigen Endgeräte steuert.

Am Mehrgeräteanschluß⁴ können direkt ISDN-fähige Apparate wie Telefone oder Faxgeräte der Gruppe 4 angeschlossen werden. Wahlweise ist auch hier der Betrieb einer Telefonanlage möglich - auch parallel zu anderen Endgeräten.



Den Mehrgeräteanschluß gibt es von der Deutschen Telekom AG⁵ wiederum in drei verschiedenen Varianten: Einfach-, Standard- und Komfortanschluß⁶. Diese unterscheiden sich nur in den zur Verfügung gestellten Leistungsmerkmalen. Welche Leistungsmerkmale die privaten Festnetzbetreiber anbieten werden, ist heute noch nicht abzusehen.

Hauptsächlich private Kunden und kleinere Firmen nutzen den ISDN-Basisanschluß. Zur Vergrößerung der Kapazität können auch mehrere Basisanschlüsse parallel an eine Telefonanlage geschaltet werden, so daß diese in Schritten von je 2 B-Kanälen beliebig erweiterbar ist.

2.2.2 Der ISDN-Primärmultiplexanschluß

Der Primärmultiplexanschluß stellt dem Benutzer 30 B-Kanäle mit einer Bandbreite von je 64 kBit/sec zur Verfügung, die von einem 64kbit/sec -D-Kanal gesteuert werden.

Ihn gibt es ausschließlich als Anlagenanschluß, so daß nicht direkt Endgeräte angeschlossen werden können, es sei denn sie nutzen die volle Bandbreite der 30 B-Kanäle von insgesamt 2Mbit/sec . Andernfalls ist zwingend eine TK-Anlage erforderlich, die die weiteren Endgeräte steuert.

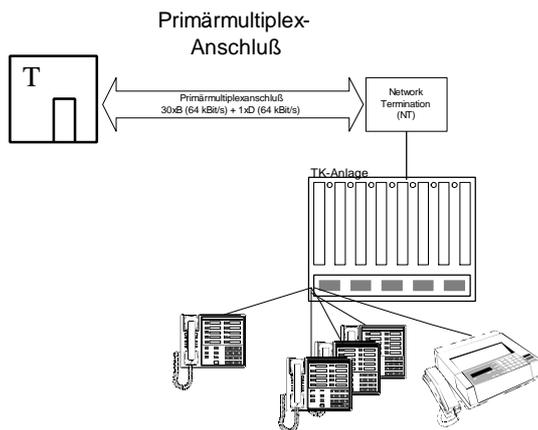
² vgl. z.B. [boe95] Abschnitt 2.1

³ auch Punkt-zu-Punkt-Verbindung genannt

⁴ auch Punkt-zu-Mehrpunkt-Verbindung genannt

⁵ Erst 1998 (Wegfall des Sprachmonopols) werden andere Anbieter hinzukommen.

⁶ vgl. [boe95]



Den Primärmultiplexanschluß nutzen größere Firmen und Institutionen, denen ein oder mehrere Basisanschlüsse nicht ausreichen, um ihre Kommunikation zu bewältigen. Auch hier kann man die Kapazität in Schritten von je 30 B-Kanälen erweitern, indem man weitere Primärmultiplexanschlüsse hinzunimmt.

Durch gleichzeitige Nutzung des gesamten Primärmultiplexanschlusses können Datenverbindungen mit einer Bandbreite von 2Mbit/sec realisiert werden.

2.2.3 Zusammenfassung

Für die weiteren Betrachtungen muß man also unterscheiden: Handelt es sich um einen Basis- oder Primärmultiplexanschluß und wird am Basisanschluß eine TK-Anlage betrieben oder nicht?

2.3 ISDN-Dienste

ISDN steht für Integrated Services Digital Network (zu deutsch: diensteintegrierendes digitales Netzwerk). Es integriert alle bisher existierenden Dienste in einem einzigen digitalen Netz. Waren bisher neben dem Fernsprechnet eigene Netze für die Datenübertragungen der Dienste Telex, Teletex, Datex-L, Datex-P, Temex etc. nötig, so können alle diese Dienste nun über ein einziges Netz angeboten werden.⁷ Hinzu kommen noch einige neue Dienste, die erst im ISDN möglich werden. Insgesamt sind folgende Dienste verfügbar:⁸

- Fernsprechen 3.1 kHz / 7 kHz
- Fax Gruppe 3 / Gruppe 4
- Daten 64 kBit/sec
- X.21 / X.25
- BTX / BTX neu
- Teletex 64
- Bild-Telefonie / Grafik-Telefonie
- Temex (Fernwirken)
- Mix-Mode

⁷ Zur Problematik der Endgeräte siehe Abschnitt 2.5

⁸ siehe [göl97]

2.4 Leistungs- und Komfortmerkmale

2.4.1 Verbindungsunabhängige Merkmale

Verbindungsunabhängige Leistungs- und Komfortmerkmale sind das elektronische Telefonbuch, die Anwahl bei aufliegenderm Hörer sowie Lauthören und Freisprechen.

Das elektronische Telefonbuch bietet dem Benutzer die Möglichkeit, Namen und dazugehörige Telefonnummern im Telefon abzuspeichern. Zum Anwählen eines bestimmten Teilnehmers wird dieser menügesteuert über seinen Namen aufgerufen und das Telefon stellt selbständig die Verbindung mit der dazugehörigen Telefonnummer her.

Die Anwahl bei aufliegenderm Hörer erlaubt es dem Benutzer, beim Verbindungsaufbau die Hände frei zu behalten und andere Arbeiten zu erledigen, bis die Verbindung erfolgreich hergestellt ist. Dieses Komfortmerkmal ist immer kombiniert mit dem Lauthören.

Das Lauthören und Freisprechen ermöglicht es dem Benutzer in Ergänzung zur Wahl bei aufliegenderm Hörer, auch beim eigentlichen Gespräch die Hände frei zu haben. Dabei unterscheidet man das reine Lauthören und das Freisprechen.

Beim reinen Lauthören wird ein im Telefon eingeschalteter Lautsprecher aktiviert, der es auch anderen Personen im Raum des Anrufers gestattet, mitzuhören. Der Gesprächspartner hört hingegen nur das, was sein unmittelbarer Gegenüber sagt.

Beim Freisprechen werden ein eingebauter Lautsprecher und ein Mikrofon aktiviert, so daß das gemeinsame Telefonieren mehrerer Gesprächspartner in einem Raum mit dem Gegenüber am anderen Ende der Leitung möglich wird.

2.4.2 Verbindungsabhängige Merkmale

Verbindungsabhängige Leistungs- und Komfortmerkmale sind die Rufnummernanzeige, Rückfragen, Makeln, Konferenz, Anklopfen und Rückruf bei Besetzt.

Die Rufnummernanzeige ermöglicht es dem Angerufenen, bereits vor dem Abheben zu erkennen, wer ihn anruft. Im Display des Telefons erscheint die Rufnummer des Angerufenen,⁹ sofern dieser das nicht ausdrücklich unterbindet.¹⁰ Ist die Nummer des Anrufers gar im elektronischen Telefonbuch des Angerufenen gespeichert, wird statt der Nummer der Name des Anrufers eingeblendet. Der Angerufene kann sich also gleich auf das Gespräch einstellen.

Rückfragen ermöglicht den Aufbau einer zweiten Verbindung, während die erste gehalten wird. Der Gesprächspartner der ersten Verbindung kann dabei das zweite Gespräch nicht hören.

Makeln bezeichnet das Umschalten zwischen zwei Verbindungen; immer eine von ihnen ist aktiv, die andere wird gehalten. Auch hier kann der gerade gehaltene Gesprächspartner das andere Gespräch nicht hören.

Eine Konferenz ermöglicht das Zusammenschalten von bis zu zehn Teilnehmern¹¹ zu einem Gespräch; dabei kann jeder jeden hören. Einer der Teilnehmer hat dabei die Aufgabe eines Konferenzleiters. Nur er kann neue Teilnehmer hinzunehmen und er zahlt die Gespräche.

⁹ CLIP - Calling Line Identification Presentation

¹⁰ CLIR - Calling Line Identification Restriction

¹¹ Bei der sogenannten „großen“ Konferenz. Es gibt auch die Dreierkonferenz.

Anklopfen verhindert das Besetztzeichen beim Anrufer. Selbst wenn der Angerufene bereits ein Gespräch führt, hört der Anrufer das Freizeichen. Im Hörer bzw. Lautsprecher des Angerufenen wird ein Aufmerksamkeitston erzeugt, der ihn auf einen weiteren Anruf hinweist. Er kann dann das erste Gespräch beenden oder durch Makeln zum anderen Teilnehmer wechseln.

Rückruf bei Besetzt erspart es dem Benutzer, einen lange besetzten Anschluß immer wieder anzuwählen. 15 Sekunden nachdem der Angerufene aufgelegt hat, wird dies dem erfolglosen Anrufer signalisiert und er kann durch Abheben des Hörers den Verbindungsaufbau einleiten.

2.5 ISDN-Endgeräte¹²

Im Folgenden werden die Endgeräte zunächst klassifiziert und ihre typischen Leistungsmerkmale beschrieben. Anschließend werden potentielle Schwachstellen aufgezeigt und erläutert.

Mit der Digitalisierung des Telefonnetzes werden auch neue, digital arbeitende Endgeräte nötig. Bereits beim Übergang vom Wählscheibentelefon zum Tastentelefon kamen sogenannte Komfortmerkmale auf. Dazu gehören die Wahlwiederholung der zuletzt gewählten Nummer, das Lauthören und das Freisprechen. Vereinzelt gab es auch Telefone mit integrierter Flüssigkristall-Anzeige (LCD), um die gewählte Nummer und den Zustand des Telefons darzustellen. Die digitalen ISDN-Endgeräte bieten alle diese Merkmale und noch einige mehr:

2.5.1 ISDN-Telefone

Digitale, ISDN-fähige Telefone sind mit diesen herkömmlichen Telefonen nicht zu vergleichen, so komfortabel sie auch gewesen sein mögen.

Ein ISDN-Telefon ist ein mikroprozessorgesteuertes, softwareprogrammiertes Gerät. Dadurch sind sie sehr flexibel. Sie verfügen meist über ein größeres Display, das neben Zahlen auch Text anzeigen kann. Die Anzeige dient zum einen einer Menüführung des Benutzers und zum anderen zur Anzeige von Verbindungsdaten. Mit Softkeys¹³ erfolgt die gesamte Programmierung und Bedienung des Telefons menügesteuert. Der Benutzer kann darüber die neuen, erst mit dem ISDN möglich gewordenen Leistungsmerkmale steuern.

Der allgemeine Trend bei ISDN-Telefonen zu mehr Benutzerkomfort hat sich auch auf die aktuelle Generation analoger Telefone übertragen. Leistungsmerkmale wie namentliches Telefonbuch, integrierter digitaler Anrufbeantworter, Tasten für Makeln und Rückfragen und Ähnliches sind immer häufiger zu finden.

2.5.2 ISDN-TK-Anlagen

In kleinen und großen Firmen und zunehmend auch in Privathaushalten haben Telekommunikationsanlagen Einzug gehalten. Sie verbinden interne und externe Kommunikation miteinander und mit den ISDN-Leistungsmerkmalen.

Von den herkömmlichen Telefonanlagen unterscheiden sie sich außerdem dadurch, daß über sie neben dem Telefonieren auch die anderen Dienste des ISDN möglich sind.

¹² Eine Übersicht findet man z.B. in [boc86] und in [boe95].

¹³ Das sind Tasten, die ihre Bedeutung ändern können. Die aktuelle Funktion wird angezeigt.

Überwiegend für den Hausgebrauch sind kleine ISDN-TK-Anlagen gedacht. Sie sind für ein bis zwei Basisanschlüsse und vier bis 16 Nebenstellen geeignet. Bei diesen Anlagen sind die Nebenstellen meist in analoger Technik gehalten, so daß vorhandene Endgeräte weiter genutzt werden können. Zusätzlich sind ein bis zwei digitale Anschlüsse¹⁴ vorhanden, an die handelsübliche ISDN-Telefone angeschlossen werden können, um das volle Spektrum der ISDN-Merkmale zu nutzen.

Davon muß man die großen ISDN-TK-Anlagen unterscheiden, die größere Firmen und Behörden betreiben. Hier können mehrere Primärmultiplexanschlüsse und einige tausend Nebenstellen vorhanden sein. Die überwiegende Zahl der Nebenstellen ist hier digital, nur ein kleiner Teil analog ausgeführt. Die verwendeten digitalen Endgeräte sind meist herstellerepezifisch. Sie lassen sich deshalb nur zusammen mit der Anlage betreiben. Für solche Anlagen wird eigenes Wartungs- und Konfigurationspersonal benötigt. Sie verfügen über Rechneranschlüsse für die Konfiguration und Auswertung der Anlagendaten und für die Gebührenabrechnung. Oft sind auch spezielle Schnittstellen für die Fernwartung vorhanden.

2.5.3 Sonstige Endgeräte

Neben den oben genannten Endgeräten gibt es noch eine Reihe weiterer. Sie lassen sich unterteilen in digitale und analoge Endgeräte.

Digitale Endgeräte wurden speziell für das ISDN geschaffen und können direkt an einen ISDN-Anschluß geschaltet werden. Dazu gehören ISDN-Telefone, ISDN-Karten für PCs und ISDN-Telefaxgeräte (Gruppe 4).

Analoge Endgeräte stammen meist aus der Zeit vor ISDN. Um sie weiterhin betreiben zu können, kann man sogenannte Terminaladapter (TA) zwischen Endgerät und ISDN-Anschluß schalten. Der Terminaladapter übersetzt die Daten und Signale zwischen dem analogen Dienst und dem ISDN.

Zu den analogen Endgeräten gehören Anrufbeantworter,¹⁵ analoge Telefone, Faxgeräte der Gruppe 3, Datex-L-, Datex-P-, Telex-, Teletex-, Temex-¹⁶ und BTX-Geräte.

2.6 Sicherheit bei ISDN-Dienstmerkmalen

Die digitale Steuerung und Signalverarbeitung im ISDN erhöht zwar ganz wesentlich den Komfort, birgt aber auch ganz neue Risiken. Das ISDN ist stärker mit klassischen Computernetzen verwandt als mit dem Vorgänger Telefonnetz. Das gilt auch für seine Angreifbarkeit. Eine Reihe von Komfortfunktionen stellen dabei eine besondere Gefahr dar. Sie werden zum besseren Verständnis zunächst beschrieben. Anschließend werden die Gefahren erläutert.

2.6.1 Leistungs- und Komfortmerkmale in TK-Anlagen

Innerhalb einer TK-Anlage stehen alle Leistungsmerkmale des ISDN-Anschlusses zur Verfügung und oft noch einige darüber hinausgehende, wie zum Beispiel Direktansprechen, Rückruf im Freifall, Nachziehen der Telefonnummer und Heranholen von Rufen.

¹⁴ sogenannter S₀-Bus

¹⁵ Es gibt heute noch keine alleinstehenden Anrufbeantworter für das ISDN. Lediglich ISDN-Telefone mit integriertem Anrufbeantworter sind im Kommen.

¹⁶ Fernwirken

Direktansprechen wird auch als Chef-Sekretär-Funktion, kurz „Chese“, bezeichnet. Dabei ersetzt die ISDN-TK-Anlage eine Gegensprechanlage. Ein Teilnehmer kann über die Freisprecheinrichtung seines Telefons mit einem anderen Teilnehmer innerhalb der Anlage sprechen. Dieser muß dazu weder den Hörer abnehmen noch das Mikrofon von sich aus aktivieren. Alles geschieht automatisch.

Der Rückruf im Freifall ergänzt den Rückruf im Besetztfall. Anlagenintern kann ein Rückrufwunsch auch dann eingeleitet werden, wenn der Gerufene nicht an seinem Platz ist. Sobald er anschließend ein Telefonat führt, weiß die Anlage, daß er wieder da ist und leitet nach Beendigung des Gesprächs den automatischen Rückruf ein.

Nachziehen der Telefonnummer ermöglicht es mobilen Teilnehmern, jeden Telefonapparat in der TK-Anlage zu ihrem eigenen zu machen. Sie geben dort ihre Benutzerkennung und Geheimzahl (PIN) ein und schon werden ihre Gespräche dorthin umgeleitet. Außerdem verfügt der Apparat dann über alle Rechte des Benutzers.

Durch das Heranholen von Rufen kann in einer Arbeitsgruppe ein beliebiger Kollege das Gespräch entgegennehmen, wenn der Gerufene gerade nicht an seinem Platz ist, ohne daß dieser seinen Apparat gezielt umleiten müßte.

2.6.2 Abhören von Räumen

Ein Raum ist prinzipiell über die Telefonleitung abhörbar, sobald sich in ihm ein Telefon mit Mikrofon befindet. Zwei ISDN-Leistungsmerkmale kommen hierfür in Frage: Das Freisprechen und das Direktansprechen.

Wenn ein Angreifer zu dem abzuhörenden Raum Zutritt hat, kann er eine Telefonverbindung zu einem beliebigen Telefon in der Welt aufbauen, wenn gerade niemand außer ihm im Raum ist. Sobald er die Freisprecheinrichtung aktiviert hat, kann der Gesprächspartner am anderen Ende der Leitung den Raum abhören, bis die bestehende Verbindung entdeckt wird oder er selbst sie auslöst.

Deshalb gibt es Vorschläge, bei aktiviertem Freisprechen in regelmäßigen Abständen ein Aufmerksamkeitston zu erzeugen. Doch auch dieser läßt sich bei zusätzlichem Zugang zur Anlage möglicherweise deaktivieren.¹⁷

Ein Angreifer braucht aber noch nicht einmal Zutritt zu dem abzuhörenden Raum, wenn das darin befindliche Telefon das Leistungsmerkmal Direktansprechen freigegeben hat. Dann kann von jedem Telefon der Anlage aus, das die Berechtigung zum Direktansprechen besitzt, das Mikrofon im abzuhörenden Raum aktiviert werden. Zwar ist auch hier ein Aufmerksamkeitston zu Beginn des Ansprechens vorgesehen, doch auch der läßt sich mit entsprechender Systemkenntnis umgehen.

2.6.3 Abhören von Telefongesprächen

Früher war ein physikalischer Zugang zu einer abzuhörenden Leitung notwendig; im ISDN reicht dafür ein Telefonanschluß und genügend kriminelle Energie.

Drei verschiedene Leistungsmerkmale ermöglichen es einem Angreifer, Telefongespräche abzuhören: Das Aufschalten, die Konferenz und die Zeugenschaltung.

Das Aufschalten ist vorgesehen, um in dringenden Fällen Telefongespräche unterbrechen und in die laufende Verbindung hinein eine Nachricht absetzen zu können. Normalerweise

¹⁷ Dazu später mehr.

se ist das Aufschalten nur wenigen Endgeräten (typischerweise der Vermittlung und eventuell der Sekretärin) erlaubt. Außerdem ist ein regelmäßig wiederkehrender Aufmerksamkeitston vorgesehen. Ein Angreifer mit Zugang zur Anlage könnte sich jedoch die benötigten Rechte verschaffen und den Aufmerksamkeitston unterbinden.

Die Konferenz birgt ein ganz anderes Risiko: Ein Teilnehmer könnte sich von den anderen Konferenzteilnehmern verabschieden, aber nicht auflegen. Er kann dann den weiteren Verlauf der Konferenz mithören, ohne daß die anderen Teilnehmer dies bemerken.¹⁸

Das Leistungsmerkmal Zeugenschaltung ermöglicht die gezielte Zuschaltung eines Dritten als Zeugen durch einen der Teilnehmer an einer Telefonverbindung. Das ist in Deutschland nicht zulässig. Da - dank Euro-ISDN- die Endgeräte aber auch in Ländern verkauft werden, wo dieses Merkmal zulässig ist und auch gefordert wird, kann man davon ausgehen, daß es auch in deutschen Telefonanlagen vorhanden ist.¹⁹

2.7 Angreifbarkeit von TK-Anlagen

Wenn man sich über die Sicherheit von TK-Anlagen Gedanken macht, muß man zwischen Angriffen durch Außentäter und durch Innentäter unterscheiden:

2.7.1 Angriffe durch Außentäter

Außenstehende haben verschiedene Möglichkeiten, in eine TK-Anlage einzudringen oder sie zu manipulieren:

Die wohl klassische Möglichkeit ist der Einbruch in den TK-Anlagen-Raum. Oftmals sind solche Räume für Außenstehende leicht zu finden²⁰ und unzureichend durch Alarmanlagen gesichert. Auch können Eindringlinge als Wartungstechniker getarnt Zugang zur Anlage oder zu Schalt- und Verteilerschränken sogar während der Geschäftszeiten erlangen.

Der Eindringling kann zusätzliche Baugruppen in der Anlage unterbringen, die vorhandenen manipulieren oder Nebenstellen mit beliebigen Berechtigungen hinzufügen.

Die zusätzlichen Baugruppen können beispielsweise Gespräche bestimmter Nebenstellen oder Fax- und Datenübertragungen abhören. Der Wirtschaftsspionage ist damit Tür und Tor geöffnet.

Die Chancen stehen gut, daß diese Baugruppen über einen längeren Zeitraum unentdeckt bleiben. In alten, analogen Anlagen wurden die mechanischen Anlagenteile wie Drehwähler in regelmäßigen Intervallen ausgetauscht. In den digitalen Anlagen wird erst jemand aktiv, wenn die Anlage selbst einen Defekt erkannt hat. Solange wird vermutlich niemand einen Blick hinein werfen.

Über zusätzliche Nebenstellen könnte unbemerkt auf Kosten des betroffenen Unternehmens kommuniziert werden²¹ oder Leistungsmerkmale benutzt werden, die für normale Apparate nicht freigegeben sind wie Aufschalten oder Direktansprechen.

Neben diesen Manipulationen an der Hardware der Anlage sind auch Softwaremanipulationen möglich:

¹⁸ vgl. [bsi94]

¹⁹ vgl. [bsi94]

²⁰ weil sie auf Lageplänen als solche gekennzeichnet werden. Siehe [bsi94]

²¹ „Gebührenbetrug“, siehe unten

Jede größere Anlage verfügt über einen Wartungs- und Bedienplatz, der meist in unmittelbarer Nähe der Anlage aufgestellt ist. Die Anlagenhersteller sichern diesen Zugang zur Anlage mit einem Paßwort ab, das aber in vielen Fällen durch den Betreiber nie geändert wird. Nach Auskunft von Insidern gibt es auch Hersteller, die für alle Anlagen das selbe, vom Kunden nicht zu ändernde Paßwort verwenden. Wer also die Standardpaßwörter der gängigen TK-Anlagen kennt, wird auch diese Hürde in vielen Fällen nehmen können.

Dann kann er zusätzliche Rufnummern einrichten, die Paßwörter für den Wartungszugang verändern, die Gebührendaten auslesen und möglicherweise verändern, Warntöne für Funktionen wie Aufschalten oder Direktansprechen manipulieren oder die Anlage durch unsinnige Konfiguration zum Absturz bringen.

Die zusätzlichen Rufnummern können von außen benutzt werden, um auf Kosten des betroffenen Unternehmens zu kommunizieren. Dazu richtet der Angreifer eine Rufumleitung zu dem Teilnehmer ein, mit dem er eigentlich telefonieren möchte. Jeder, der später diesen Anschluß anwählt, wird auf Kosten des Unternehmens weiterverbunden.

Mit Hilfe des Paßworts für den Fernwartungszugang²² steht die gesamte Anlage wiederholbar offen, ohne daß erneut jemand persönlich eindringen müßte. Alle weiteren Einbrüche können dann von jedem Telefon der Welt aus geschehen. Damit sinkt das Risiko, entdeckt zu werden.

Die Gebührendaten können im Zusammenhang mit Wirtschaftsspionage oder zur Erstellung von Kommunikationsprofilen mißbraucht werden.²³

Das Abschalten der Warntöne beim Aufschalten oder Direktansprechen macht diese Leistungsmerkmale zu den kritischsten innerhalb einer TK-Anlage. Denn damit können Räume oder Gespräche unbemerkt abgehört werden. Oft lassen sich die Warntöne per Programmierung nicht abschalten, aber die Lautstärke, Dauer oder Tonfrequenz lassen sich so verändern, daß die Töne nicht mehr wahrgenommen werden.

Das unsinnige Umprogrammieren der Anlage hat zum Ziel, sie zum Abstürzen zu bringen. Bis zur Wiederherstellung des ursprünglichen Zustands können die Anlagenbenutzer nicht mehr telefonieren, keine Faxe senden und empfangen und keine Daten mit Anderen austauschen. Diese Art der Manipulation gehört ebenso wie sonstige Sabotage zu den Anschlägen:

Viele Unternehmen hängen heute essentiell von ihrer Telekommunikations-Infrastruktur ab. Ein Ausfall der TK-Anlage schon für wenige Stunden oder Tage kann einem Unternehmen das Genick brechen.²⁴

Deshalb stellt die Hard- und Software der TK-Anlage einen kritischen Angriffspunkt dar. Über Manipulationen an der Software kann die gesamte Anlage in einen unsinnigen Zustand gebracht werden, so daß sie erst nach einem Neustart wieder zu benutzen ist. Schlimmstenfalls müssen vor dem Neustart Sicherungen der Anlagenkonfigurations-Daten wieder eingespielt werden. Der gesamte Vorgang kann so Stunden bis Tage in Anspruch nehmen.

Schlimmer kann ein Unternehmen die physikalische Zerstörung der Anlage oder von Anlagenteilen treffen. Ein Feuer, eindringendes Wasser oder Überspannung an Anlagen-

²² zum Fernwartungszugang siehe Abschnitt 2.7.1.1

²³ siehe Abschnitt 2.7.3

²⁴ vgl. [bsi94]

Baugruppen legen mindestens diese Teile bis zum Austausch mit anschließendem Neustart der gesamten Anlage lahm.

Ein Feuer im Kabel-Rangierraum²⁵ kann nach Auskunft von Fachleuten eine Anlage mehrere Wochen lahmlegen. Ähnliche Auswirkungen kann bereits das Durchtrennen wichtiger Kabelstränge in diesem Raum oder in angrenzenden Kabelschächten haben.

2.7.1.1 Fernwartungszugang

Moderne Anlagen bieten die Möglichkeit, über eine bestimmte Nebenstellenummer administriert zu werden, ohne daß ein Techniker anwesend sein muß. Gerade für mittelgroße TK-Anlagen lohnt sich ein eigener Techniker nicht und einen Techniker des Herstellers anreisen zu lassen ist teuer. Diese Unternehmen kaufen dann beim Hersteller die Dienstleistung der Fernwartung ein.

Größere Unternehmen haben zwar in der Regel eigene Techniker, die befinden sich aber oft nur an einem Standort. Um die TK-Anlagen in den Niederlassungen mit zu warten, bietet sich auch hier ein Fernwartungszugang an.

Derselbe Zugang, der berechtigten Technikern die Anlage öffnet, kann aber auch von unberechtigten Eindringlingen mißbraucht werden. Deshalb sollte jedes Unternehmen prüfen, ob es zugunsten der Sicherheit nicht ganz auf die Fernwartung verzichtet oder den Fernwartungszugang nur innerhalb des Firmennetzes verfügbar macht.

Den besten Kompromiß zwischen Komfort, Kosten und Sicherheit stellt die Fernwartung mit Call-Back-Lösung dar. Dabei ruft der Wartungstechniker die zu wartende Anlage an; diese erkennt den Wartungswunsch, trennt die Verbindung und ruft die ihr bekannte Nummer des Wartungsplatzes zurück. Erst dann erlaubt sie den Zugriff auf die Anlagendaten.

Doch auch beim Einsatz des Call-Back-Verfahrens bleibt ein nicht zu unterschätzendes Restrisiko. Wenn der Anlagenbetreiber dem Anlagenhersteller die Administration der Anlage überläßt, hat er keine Möglichkeit, die Konfiguration zu prüfen. Ein prinzipiell berechtigter Wartungstechniker könnte also durch Bestechung dazu gebracht werden, die Anlage eines Kunden zu manipulieren, so daß der oben beschriebene Mißbrauch möglich ist, ohne selbst in die Anlage einzudringen.

2.7.1.2 Angriffe über den D-Kanal

Über den D-Kanal kann ein Angreifer von außen unsinnige oder manipulierende Kommandos an eine TK-Anlage schicken. Wenn diese sie ungefiltert an die Endgeräte weiterleitet, besteht eine große Sicherheitslücke. Dann könnten beispielsweise von jedem Telefonapparat der Welt beliebige Räume oder Telefonate abgehört werden. Es wäre nicht mehr notwendig, in das abzuhörende Unternehmen einzudringen.

Eine Lösung für dieses Problem stellt die D-Kanal-Firewall dar, die analog zu Firewalls in Rechnernetzen wie dem Internet die ankommenden Datenpakete filtert. Nur für unkritisch befundene Datenpakete werden durchgelassen.

Der D-Kanal selbst und seine Sicherheitslücken werden im nächsten Kapitel ausführlich beschrieben; der Firewall-Ansatz wird in Kapitel 8 näher untersucht.

²⁵ dort werden die Teilnehmerleitungen physikalisch auf die Anlage aufgeschaltet

2.7.2 Angriffe durch Innentäter

Firmenangehörige können ebenso wie Außentäter versuchen, die TK-Anlage zu kompromittieren. Das größte Risiko stellen diejenigen dar, die Privilegien in der Anlage haben. Das sind die Servicetechniker und die Vermittlungskräfte.

Die Servicetechniker können sich und anderen Nutzern Nebenstellen so einrichten wie sie möchten. Die Berechtigung, internationale Gespräche zu führen ist damit ebenso möglich, wie die Berechtigung zum Umschalten auf Verbindungen oder für das Direktansprechen. Außerdem können sie eine Manipulation der Gebührendaten vornehmen oder zulassen. Und sie können eine unbenutzte Durchwahlnummer ins Ausland umleiten, so daß auf Kosten des Anlagenbetreibers dorthin telefoniert werden kann.

Die Vermittlungskräfte können den Benutzern von Nebenstellen entgegen etwaigen Arbeitsanweisungen internationale Gespräche ermöglichen. Sie verfügen außerdem in der Regel über das Recht, sich auf eine bestehende Verbindung aufzuschalten. Dies dient eigentlich dazu, besonders dringende Anrufe zu signalisieren, wenn bereits mit einem anderen Teilnehmer gesprochen wird, kann aber zum Abhören von Gesprächen mißbraucht werden.

Aber auch die Nebenstelleneinhaber sind potentielle Angreifer von Innen. Falls sie über eine entsprechende Berechtigung verfügen, können auch sie eine Rufumleitung ins Ausland programmieren, die dann von Außenstehenden mißbraucht wird.

2.7.3 Kommunikationsprofile

In ISDN-Anlagen ist es häufig notwendig, folgende Verbindungsdaten zu Abrechnungszwecken für einen Zeitraum von mehreren Wochen zwischenspeichern:

- Datum, Uhrzeit des Anrufs
- rufende Nebenstelle
- angewählte Nummer
- Dauer des Gesprächs
- entstandene Gebühren

Da die Abrechnung der Gebühren EDV-gestützt abläuft, werden die Daten in Rechneranlagen zwischengespeichert und verarbeitet. Damit ist es möglich, das Kommunikationsverhalten einzelner oder aller Teilnehmer rechnerunterstützt zu analysieren. Das hat zum einen datenschutzrechtlich eine Bedeutung, weil es zu einer Überwachung der Mitarbeiter führen kann. Allein die Möglichkeit läßt schon einen Vertrauensverlust zwischen Unternehmen und Mitarbeiter befürchten.

Zum anderen können die Daten von Außenstehenden mißbraucht werden. Sie können daraus die Intensität der Geschäftsbeziehungen mit anderen Unternehmen ablesen. Das kann für die Konkurrenz durchaus eine wertvolle Information sein. Außerdem könnten Mitarbeiter erpreßbar werden, wenn zum Beispiel aus ihren Gesprächsprofilen hervorgeht, daß sie regelmäßige Telefonate mit ihrer Geliebten führen.

2.7.4 Fazit

Wenn es einem Angreifer erst einmal gelungen ist, eine ISDN-Anlage unter Kontrolle zu bringen, wird es in der Regel eine ganze Weile dauern, bis seine Machenschaften entdeckt werden. Dazu trägt bei, daß er unter Umständen gar nicht oder nur einmal physikalisch eindringen muß. Alle weiteren Manipulationen können aus der sicheren Ferne erfolgen.

Nutzt er die Anlage für kostenlose Gespräche im großen Stil, wird er nach der nächsten Rechnung auffliegen. Aber das kann schon einmal sechs bis acht Wochen dauern.

Andere Manipulationen können noch länger unentdeckt bleiben. Das liegt an der Komplexität größerer Anlagen. Kein Mensch ist in der Lage, eine große TK-Anlage mit ihren Hardwarekomponenten und den freigeschalteten Dienst- und Leistungsmerkmalen zu überblicken. Und mit jedem Software-Update, das vorhandene Probleme löst, kauft man sich mehrere neue ein. Das Ziel der Wartungstechniker muß es sein, diese zu finden, bevor es ein Anderer tut.

Computerunterstützung gibt es für diese Tätigkeit leider (noch) nicht.

Man könnte sich aber vorstellen, ein Pendant zu „Satan“ zu schaffen. Satan²⁶ ist ein Programm, das gängige Sicherheitslücken in UNIX-Rechnern kennt und einen Zielrechner systematisch mit Hilfe dieser Kenntnis angreift. Anschließend generiert es einen Bericht der gefundenen Lücken. Es ist eine übliche Methode, sich die Mittel und das Wissen der potentiellen Angreifer zu besorgen und sich selbst anzugreifen, um so Lücken aufzudecken. Damit kann man Lücken schließen bevor Angreifer sie ausnutzen. Es gibt aber auch Lücken, die sich nicht ohne weiteres schließen lassen, weil sie in der Verantwortung des Anlagenherstellers oder des Netzbetreibers liegen. Auf sie können die Verantwortlichen aber zumindest besonderes Augenmerk richten.

Unter Umständen muß man aus Sicherheitsgründen auf einige komfortable aber unsichere Leistungsmerkmale verzichten. Dazu werden sie anlagenweit gesperrt. Das Wartungspersonal muß dann regelmäßig prüfen, daß die Sperrung noch aktiv ist, um einen heimlichen Mißbrauch durch Umprogrammieren auszuschließen.

2.8 ISDN-vernetzte Rechner

ISDN-Leitungen werden wegen ihrer relativ hohen Bandbreite von 64 kBit/sec je B-Kanal zunehmend auch zur Rechnervernetzung verwendet. Insbesondere Rechenzentren stellen ISDN-Zugänge bereit, über die die Anrufer ihre Daten übertragen können.

So manches Rechenzentrum benutzt dabei die Rufnummernübermittlung²⁷ als Identifizierung des Anrufers und verzichtet auf weitere Sicherheitsabfragen. Das kann aber gefährlich werden. Wie im nächsten Kapitel über das D-Kanal-Protokoll gezeigt, kann eine Rufnummer übermittelt werden, die vom Netz nicht geprüft wurde. Damit ist es möglich, von überall in dieses Rechenzentrum einzudringen, indem eine berechnete Rufnummer vorgetäuscht wird.

Deshalb kann auf keinen Fall auf weitere Sicherheitsabfragen oder auf Call-Back verzichtet werden. Beim Call-Back-Verfahren wird durch den Anruf im Rechenzentrum nur der Verbindungswunsch von einer bestimmten Telefonnummer aus signalisiert. Die Verbindung wird sofort unterbrochen und die übermittelte Nummer zurückgerufen. Erst dann wird die eigentliche Verbindung aufgebaut.

Eine andere Möglichkeit, die Rechnerkommunikation über das ISDN sicherer zu machen, ist die geschlossene Benutzergruppe (GBG, CUG²⁸). Dieses Dienstmerkmal erlaubt es, für einen ISDN-Anschluß festzulegen, mit wem er kommend und gehend kommuni-

²⁶ http://web.indstate.edu/~cckeg/security/satan/satan_documentation.html

²⁷ CLIP - Calling Line Identification Presentation

²⁸ Closed User Group

zieren darf. Die GBG kann dabei für jede Dienstekennung individuell eingestellt werden. So kann ein Basisanschluß beispielsweise so eingerichtet werden, daß der Benutzer mit jedem anderen Anschluß telefonieren, aber nur mit ganz bestimmten Anschlüssen Daten austauschen darf.

Dadurch läßt sich beispielsweise auch der Fernwartungszugang zusätzlich absichern: Nur berechnete Fernwartplätze erhalten Zugriff auf den Anschluß.

Aber gerade weil die GBG für einzelne Dienstekennungen getrennt aktiviert werden kann, ist sie unsicher: Durch eine einfache Manipulation der Dienstekennung ist es beispielsweise möglich, doch eine Datenverbindung aus einem Unternehmen heraus aufzubauen und Daten nach außen zu leiten, die sicher geglaubt werden.

2.9 Zusammenfassung

Gerade für die Betreiber großer Telefonanlagen hat das ISDN Komfortverbesserungen gebracht: Die Rechte der einzelnen Nebenstellen sind frei programmierbar, den Vermittlungskräften steht ein Computer mit elektronischem Telefonbuch zur Verfügung, die Abrechnung der Gebühren erfolgt mit Computerhilfe, durch Anrufumleitung gehen weniger Gespräche verloren und neue Funktionen lassen sich relativ leicht in die bestehende Anlage integrieren.

Aber damit verbunden kauft man sich Risiken ein. Die Schwachstellen können dadurch umgangen werden, daß man sich ihrer bewußt wird und sie systematisch bekämpft. Teilweise sind hier die Anlagenhersteller, teilweise die Betreiber gefragt.

3 Der D-Kanal und die Vermittlungsstellen

3.1 Einleitung

Im letzten Kapitel wurden die Angriffspunkte in Endgeräten und innerhalb von TK-Anlagen beschrieben. Der mögliche Schaden ist dort zunächst auf *einen* Benutzer beziehungsweise auf *einen* Betreiber beschränkt.

Der nun betrachtete D-Kanal hat eine größere Reichweite und damit ein größeres Schadenspotential.

Jeder ISDN-Anschluß verfügt neben den B-Kanälen (Nutzkanäle) auch über einen oder mehrere D-Kanäle. Über diese werden Informationen für die Steuerung der B-Kanäle übermittelt.

3.2 Der ISDN-D-Kanal

Das gesamte ISDN-Protokoll ist sauber nach dem ISO/OSI-7-Schichten-Modell aufgebaut. Die unteren drei Schichten stellen zusammen das D-Kanal-Protokoll²⁹ dar. Die darüberliegenden Schichten sind abhängig vom verwendeten Dienst im B-Kanal. Bei der transparenten 64 kBit/sec-Datenübertragung sind sie nicht genormt, bei Diensten, für die es spezielle Endgeräte gibt (Telefax Gruppe 4, Bildtelefon etc.) müssen sie genormt sein.

3.3 Aufgaben des D-Kanals

Im heute noch bestehenden analogen Fernsprechnetzz werden die Steuerungsinformationen auf zwei verschiedene Weisen ausgetauscht:

Im völlig analogen System werden Wahlinformationen und das Abheben und Auflegen des Hörers über Kurzschluß/Unterbrechung der Leitung signalisiert. Im analogen System mit digitalisierten Vermittlungsstellen kommt auch das Tonwahlverfahren zum Einsatz. Dabei wird eine zu wählende Ziffer durch die Kombination aus zwei verschiedenen Tönen dargestellt. Dies geschieht aber in jedem Fall im „Sprachkanal“ - einen anderen gibt es im analogen Netz nämlich nicht.

Wegen der damit verbundenen Nachteile hat man sich im ISDN von dieser „inband“-Signalisierung verabschiedet und ist zur „outband“-Signalisierung übergegangen. Im eigens dafür geschaffenen D-Kanal werden die Informationen zur Steuerung einer Verbindung zwischen Endgerät und Vermittlungsstelle übertragen. Daneben werden große Mengen unterschiedlicher Informationen ausgetauscht. Das hängt zum einen mit der Integration der verschiedenen Dienste³⁰ zu einem einzigen Netz und zum anderen mit den dort zusätzlich angebotenen Komfortmerkmalen zusammen. Gemeinsam verursachen sie ein so hohes Datenaufkommen, daß man sich entschied, einen eigenen Kanal, den D-Kanal einzusetzen. Damit stehen die B-Kanäle in voller Bandbreite von 64kBit/sec für den Benutzer zur Verfügung. Außerdem können so Steuerinformationen übertragen werden, ohne gleichzeitig einen B-Kanal zu belegen.³¹

²⁹ E-DSS-1 oder DSS-1: (Euro) Digital Subscriber Signalling System No. 1

³⁰ siehe Kapitel 2

³¹ verbindungslos, siehe Abschnitt 3.4.3

3.4 Aufbau des D-Kanals³²

3.4.1 Schicht 1 - physikalische Schicht

Die „physikalische Schicht“ legt fest, wie die Signale elektrisch oder über eine Glasfaserleitung übertragen werden. Sie beschreibt, wie einzelne Bits über eine physikalische Leitung zu übertragen sind.

3.4.2 Schicht 2 - Sicherungsschicht

Die „Sicherungsschicht“ regelt die Paketisierung der Datenströme, die quitierte und die unquitierte Nachrichtenübermittlung und die Fehlerkorrektur. Sie ist für das *wie* der Steuerung zuständig und wurde in den Normen ITU-T Q.920³³ und Q.921³⁴ international festgelegt.

3.4.3 Schicht 3 - Vermittlungsschicht

Die „Vermittlungsschicht“ stellt einzelne Funktionen und Parameter bereit, die für die Steuerung der B-Kanäle benötigt werden. Sie wurde in ITU-T Q.931³⁵ und Q.932³⁶ genormt und regelt, *was* zur Steuerung übertragen wird. Dazu gehören zum Beispiel die gewählten Ziffern, Signalisierung ankommender Rufe und die Übertragung von Gebührendaten.

Die Nachrichten der Schicht 3 lassen sich in zwei Klassen teilen:³⁷

Die *verbindungsorientierten* Nachrichten werden verwendet, um einen B-Kanal zu steuern. Dazu gehören Nachrichten für

- Verbindungsauf- und abbau
- allgemeine Anwendungen
- verbindungsabhängige Dienstmerkmale³⁸
- die Endgeräte-Portabilität
- Zustandsanzeige
- Teilnehmer-zu-Teilnehmer-Information.

Die *verbindungslosen* Nachrichten werden unabhängig von einem B-Kanal verwendet, um Informationen zwischen Teilnehmeranschluß und Vermittlungsstelle auszutauschen. Dazu gehören Nachrichten für

- verbindungsunabhängige Dienstmerkmale³⁹ (z.B. Rufumleitung)
- Dienstmerkmalabfragen
- Editierfunktionen.

³² vgl. z.B. [kah92] oder [ban95]

³³ Q.920 (=CCITT I440): „Allgemeine Aspekte des D-Kanal-Protokolls, Schicht 2“

³⁴ Q.921 (=CCITT I441): „D-Kanal-Protokoll, Schicht 2 Spezifikation“

³⁵ Q.931: „D-Kanal-Protokoll, Schicht 3-Spezifikation“

³⁶ Q.932: „D-Kanal-Protok., Schicht 3, Allg. Prozeduren z. Steuern v. Dienstmerkmalen“

³⁷ aus [kah92], Abschnitt 4.3.2.3.

³⁸ siehe Abschnitt 2.4.2

³⁹ siehe Abschnitt 2.4.1

3.4.4 Bitfehlerrate

Durch störende Umwelteinflüsse - aber auch durch Manipulation an den Leitungen - können die Daten bei der Übertragung verfälscht werden. In der Schicht 2 des D-Kanal-Protokolls werden geeignete Maßnahmen eingesetzt, um solche Fehler zu erkennen.⁴⁰

Die Schicht 1 gewährleistet nach offiziellen Aussagen ohne Fehlererkennung eine Bitfehlerrate von 10^{-6} . Wenn doch einmal ein Fehler auftritt, wird dieser mit einer Wahrscheinlichkeit von nur 10^{-5} in der Schicht 2 nicht erkannt und korrigiert. Dadurch gewährleistet sie als Dienstleister für die Schicht 3 eine Bitfehlerrate von 10^{-11} . Das heißt, in einem B-Kanal tritt im Mittel alle 15 Sekunden ein Bitfehler auf. Aber nur jeder hunderttausendste Fehler wird nicht erkannt. Bei einer Standleitung ist das im Mittel ein Bit alle 17 Tage. Diese verbleibenden Fehler müssen in einer höheren Schicht durch Prüfsummen oder ähnliches erkannt und abgefangen werden.

Übersteigt die Bitfehlerrate 10^{-2} über einen Zeitraum von zehn Sekunden, so schaltet die Vermittlungsstelle den betroffenen Anschluß automatisch ab. Er wird dann von einem Servicetechniker geprüft.

3.5 Reichweite des D-Kanals

Gemäß CCITT⁴¹ kann man für das D-Kanal-Protokoll folgende Einsatzgebiete unterscheiden:⁴²

3.5.1 Punkt-zu-Punkt-Verbindung

Dabei wird an beiden Enden der Leitung nur je ein Endgerät angeschlossen. Die beiden haben also die Leitung exklusiv für sich. Eine solche Verbindung wird für (meist große) TK-Anlagen und für die Verbindung von Rechnernetzwerken verwendet.

3.5.2 Punkt-zu-Mehrpunkt-Verbindung

Dabei wird an einem Ende der Leitung nur ein Gerät angeschlossen. Das kann die Vermittlung oder eine TK-Anlage sein. Am anderen Ende können an einem passiven Bus bis zu acht Endgeräte angeschlossen werden. Da sich die Endgeräte die Leitung teilen, ist ein Unterscheidungsmechanismus notwendig: Jedes Endgerät bekommt eine eindeutige Adresse⁴³ zugewiesen. Diese Konfiguration wird beim Basisanschluß oder innerhalb von TK-Anlagen verwendet.

3.5.3 Zwischen der Vermittlungsstelle und dem Endgerät

Bei beiden oben genannten Verbindungstypen kann die Ortsvermittlungsstelle des Netzbetreibers auf der einen Seite der Verbindung stehen. Sie ist immer alleine an die Leitung angeschaltet. Am anderen Ende können sich ein oder mehrere Endgeräte befinden.

⁴⁰ vgl. [kah92] Abschnitte 4.2.5. und 3.8, 3.9

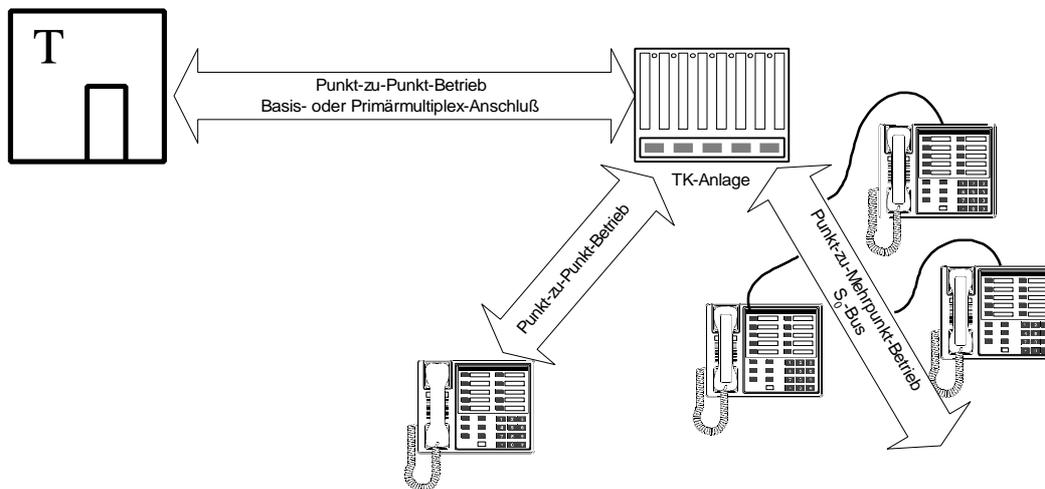
⁴¹ CCITT = Comité Consultatif International Télégraphique et Téléphonique

⁴² vgl. [kah92] Abschnitt 4.1.2 „Referenzkonfiguration für das D-Kanal-Protokoll“

⁴³ TEI: Terminal Endpoint Identifier

3.5.4 Zwischen der TK-Anlage und dem Endgerät

Große TK-Anlagen sind im Prinzip ein Abbild einer (Orts-)Vermittlungsstelle. Sie können deshalb in beiden Verbindungstypen an die Stelle der Ortsvermittlung treten. Dann tritt folgende Konfiguration auf:



Hierbei gibt es auf einer Seite einer Verbindung *zweimal* einen D-Kanal: Zwischen der Ortsvermittlung und der TK-Anlage und zwischen der TK-Anlage und dem Endgerät. Die TK-Anlage kann entweder die D-Kanal-Pakete von der Ortsvermittlungsstelle auf den internen D-Kanal durchreichen⁴⁴ oder selbst die dort benötigten Pakete generieren.⁴⁵

3.5.5 Auf einem 16 (D_{16}) oder 64 kBit-D-Kanal (D_{64})

Alle oben geschilderten Kombinationen können über einen 16 oder einen 64 kBit/sec breiten D-Kanal arbeiten. Dabei gehört zu einem Basisanschluß mit zwei B-Kanälen ein 16 kBit/sec breiter D-Kanal, zu einem Primärmultiplexanschluß mit 30 B-Kanälen einer mit 64 kBit/sec Übertragungskapazität. Diese verhältnismäßig hohe Kapazität wird aber nur selten - zum Beispiel beim Verbindungsaufbau - voll genutzt.

Deshalb ist auch die Übertragung von Nutzinformationen über den D-Kanal vorgesehen. Damit lassen sich zum Beispiel Datex-P⁴⁶ oder Temex-⁴⁷ Anwendungen realisieren.

Innerhalb einer Kommunikationsbeziehung sind die oben genannten Konfigurationen beliebig kombinierbar. So kann beispielsweise ein Teilnehmer an einer ISDN-TK-Anlage über das ISDN einen Teilnehmer an einem Basisanschluß anwählen. Denn der D-Kanal existiert auf beiden Seiten einer Verbindung nur zwischen Benutzer und der dazugehörigen Ortsvermittlungsstelle. Er ist also kein durchgehender Kanal von einem Ende der Verbindung zum anderen. Zwischen den Vermittlungsstellen werden die Steuerungsinformationen über das Zeichengabesystem (ZGS)-7-Netz ausgetauscht. Das ZGS-7 ist Thema des nächsten Kapitels.

⁴⁴ Zu den Gefahren, die daraus entstehen siehe Abschnitt 8.4.

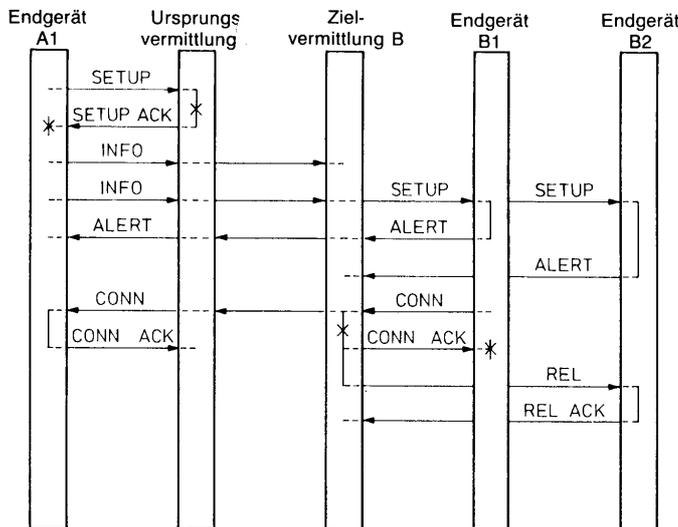
⁴⁵ Zur Problematik des D-Kanal-Filters siehe Kapitel 8.

⁴⁶ Paketorientierte Datenübertragung mit maximal 9600 Bit/sec

⁴⁷ Fernwirken

3.6 Ablauf eines Telefonats aus Sicht des D-Kanals

Das folgende Bild zeigt den Ablauf im D-Kanal beim Aufbau einer Verbindung zwischen zwei Teilnehmern. Zahlreiche Nachrichten werden zwischen dem A-Teilnehmer⁴⁸ und seiner Vermittlungsstelle, zwischen dem B-Teilnehmer und seiner Vermittlungsstelle sowie zwischen den beteiligten Vermittlungsstellen ausgetauscht:



*, Symbol für »B-Kanal durchschalten«

Bild 4-16: Verbindungsaufbau beim Mehrgeräteanschluß

aus: [kah92] Seite 162

- Der Benutzer am Endgerät A1 nimmt den Hörer ab
- A1 sendet „SETUP“ auf dem D-Kanal
- Seine Vermittlungsstelle ist bereit und antwortet mit „SETUP ACKnowledge“
- gleichzeitig wird ein B-Kanal zwischen A1 und UrsprungsVSt geschaltet
- Der Benutzer an A1 gibt nacheinander die Ziffern ein
- Das Endgerät A1 sendet sie in „INFO“-Nachrichten verpackt
- Wenn genügend Ziffern vorliegen, wird die Zielvermittlungsstelle informiert
- Sie schickt ein „SETUP“ zu allen Endgeräten bei Teilnehmer B
- Die Geräte klingeln und teilen dies der Vermittlungsstelle mit („ALERT“)
- Am Endgerät B1 wird der Hörer abgenommen
- Es sendet „CONNect“, um die Verbindung von der VSt anzufordern
- Die Zielvermittlungsstelle sendet „CONNect ACKnowledge“ zu B1
- und „RELease“ zu B2
- B2 hört auf zu klingeln und bestätigt mit „RELease ACKnowledge“
- Die Zielvermittlungsstelle informiert die Ursprungsvermittlungsstelle
- Diese sendet „CONNect“ zum Endgerät A1
- Das antwortet mit „CONNect ACKnowledge“
- Der B-Kanal ist nun durchgeschaltet, die beiden Endgeräte kommunizieren

3.7 Angriffe auf den D-Kanal

Durch die neue „outband“-Signalisierung⁴⁹ sind einige der Angriffe auf das Telefonnetz schwieriger geworden. Im analogen Netz hatten zahlreiche Kriminelle mit dem beliebten

⁴⁸ A-Teilnehmer ist immer der Anrufer, B-Teilnehmer der Angerufene

⁴⁹ siehe Abschnitt 3.3

„blue-boxing“ und mit sogenannten auto-dialern Erfolg. Das blue-boxing wird im nächsten Kapitel beschrieben, auto-dialer in Abschnitt 3.9.8.

Im Folgenden werden einzelne Angriffe wie Abhören und Aufschalten beschrieben.

3.7.1 Abhören

Im analogen Netz braucht man dafür nur einen handelsüblichen Telefonapparat, dessen Kabelenden man mit Krokodilklemmen versieht. Damit kann man sich an irgendeiner Stelle zwischen Telefonkunde und Vermittlungsstelle auf die Leitung aufschalten, mithören und auch selbst telefonieren.

Zum Aufklemmen auf einen ISDN-Anschluß braucht man wegen des dort verwendeten Echokompensationsverfahrens schon ausgefeiltere Technik

Das Echokompensationsverfahren⁵⁰:

Eine zentrale Vorgabe bei der Einführung des ISDN in Deutschland war, die vorhandenen Teilnehmeranschlußleitungen weiterhin verwenden zu können. In den Zeiten der analogen Technik wurden von den Ortsvermittlungsstellen zu den Teilnehmern zwei Kupferdrähte verlegt. Damit man bei Einführung des ISDN nicht die gesamte Verkabelung erneuern mußte, hat man sich für den Einsatz des Echokompensationsverfahrens entschieden.

Beim Anschalten des Netzabschlusses⁵¹ an die Vermittlungsstelle synchronisieren sich die beiden. Ab dann zieht jede Seite vom Empfangenen Signal den gerade selbst gesendeten Teil ab und erhält so das Signal der Gegenstelle.

Das Signal, das sich gerade auf der Leitung befindet hängt also immer von dem vorher gesendeten ab - außer im Anfangszustand.

Die Einführung des Echokompensationsverfahrens ist der Grund, weshalb beim Basisanschluß auf Teilnehmerseite ein Netzabschluß installiert werden muß: Er führt die aufwendige Echokompensation durch. Ab dem NT wird die weitere Installation vieradrig ausgeführt (der sogenannte S_0 -Bus), so daß je zwei Adern für beide Richtungen zur Verfügung stehen.

Mit speziellen Abhöreinrichtungen kann man sich hochohmig auf die Leitung aufschalten und mithören. Um das Signal richtig interpretieren zu können, muß man die Verbindung in den Anfangszustand versetzen. Dazu kann man kurz die Leitung unterbrechen. Wenn gerade kein B-Kanal in Benutzung ist, bleibt die Unterbrechung unentdeckt.

Möglicherweise kann man sich auch aufsynchronisieren, ohne die Leitung zu unterbrechen. Da bestimmte Bitfolgen nur in einer Richtung, andere nur in der anderen Richtung auftreten und der Ablauf eines Verbindungsaufbaus genormt ist, reicht es möglicherweise, eine Weile zu lauschen, um dann alle folgenden Nachrichten verstehen zu können.

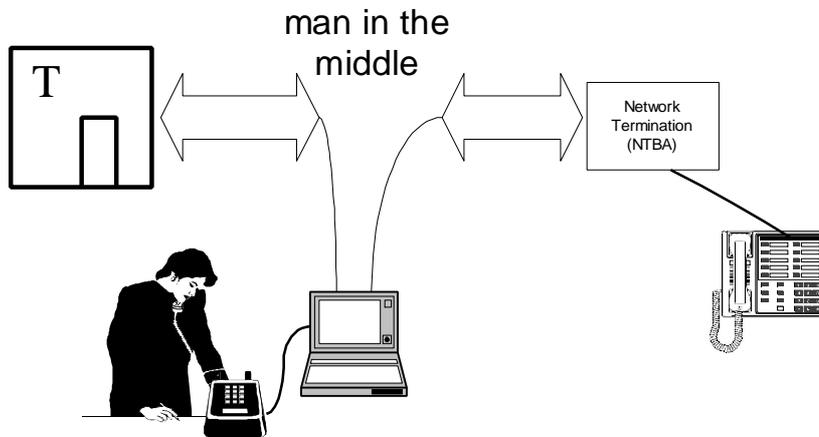
Wenn man allerdings in das Geschehen auf der Leitung aktiv eingreifen will, muß man die Leitung auftrennen und sich selbst als neues Leitungsende mit einem NT und ISDN-Endgerät oder mit einem Prüftelefon wie dem PrTel 93i⁵² aufschalten. Dann kann der Teilnehmer aber nicht mehr selbst kommunizieren.

⁵⁰ vgl.[kah92] Abschnitt 3.3.5

⁵¹ Network Terminator (NT)

⁵² siehe [ost96]

Mit Hilfe noch ausgefeilterer Technik kann man sich womöglich auch in eine bestehende Verbindung hineinschalten und manipulieren. Man spielt dann nach der man-in-the-middle-Methode beiden Seiten die jeweils andere vor:



Wenn es einem Angreifer erst einmal gelungen ist, sich so zwischen Vermittlungsstelle und Teilnehmer zu schalten, kann er beliebige Pakete auf dem D-Kanal erzeugen und diese an den Teilnehmer oder die Vermittlungsstelle schicken.

In Richtung der Vermittlungsstelle kann der Angreifer alles, was auch der Teilnehmer könnte: Er kann auf dessen Kosten und unter dessen Kennung (Rufnummer) telefonieren oder Daten übertragen, Rufumleitungen einrichten oder verändern und in begrenztem Umfang den Teilnehmeranschluß umkonfigurieren.

In der anderen Richtung kann der Angreifer alles, was die Vermittlungsstelle in Richtung Teilnehmer auch kann: Er kann beispielsweise ankommende Gespräche mit beliebiger Anrufernummer erzeugen.

Darüber hinaus kann er auch Pakete schicken, die die Vermittlungsstelle nie erzeugen würde, weil sie unsinnig oder unzulässig sind. Da die Endgeräte damit nicht rechnen, kann er sie so in einen Zustand bringen, der normalerweise nicht vorgesehen ist. Damit lassen sich möglicherweise Räume oder Gespräche abhören oder Ähnliches.

3.7.2 Abhören des Busses

Die Verkabelung ab dem network terminator (NT) ist in Vierdraht-Technik als Bus ausgeführt. An diesen Bus werden die einzelnen Endgeräte - gegebenenfalls über einen Terminaladapter - angeschlossen.

Auf dem Bus werden die beiden B-Kanäle und der D-Kanal im Zeitscheibenverfahren übertragen. Die Endgeräte hören ständig auf dem D-Kanal mit, um für sie bestimmte Pakete zu empfangen und - beispielsweise bei einem Anruf - darauf zu reagieren.

Mit Hilfe eines modifizierten Endgeräts kann man den Bus vollständig abhören und auswerten. So ist es zum Beispiel möglich, alle kommenden und gehenden Anrufe eines Endgeräts zu protokollieren - mit Datum, Uhrzeit und vollständiger(!) Nummer des Gesprächsteilnehmers. Darüber hinaus kann man auch den Inhalt der beiden B-Kanäle abhören und aufzeichnen.

Die Firma Siemens bietet beispielsweise ein Gerät namens DataVoice⁵³ an, mit dem bis zu 32 B-Kanäle gleichzeitig aufgezeichnet und archiviert werden können. Sein eigentli-

⁵³ in Siemens TelcomReport 3/96 „Manipulation ausgeschlossen“ Peter Giese und Bernd Sommer

ches Einsatzgebiet liegt bei Notrufabfragestellen der Polizei, der Feuerwehr und der Rettungsdienste. Doch darauf ist es natürlich nicht beschränkt. Dem Mißbrauch sind dank der digitalen Technik keine Grenzen gesetzt. Einzige Voraussetzung ist Zugriff auf den Bus zwischen dem NT und den Endgeräten.

Im Internet sind kostenlose Programme erhältlich, mit denen man den D-Kanal eines S₀-Bus protokollieren kann. Man benötigt nur eine ISDN-Karte für den PC, die am betreffenden Bus angeschlossen wird. Dann werden alle kommenden und gehenden Gespräche aufgezeichnet und lassen sich mit dem PC komfortabel auswerten.

Neben diesen Angriffen auf den D-Kanal sind auch Angriffe *über* den D-Kanal auf die Vermittlungsstelle oder auf die daran angeschlossenen Endgeräte einzelner Anschlüsse möglich. Sie werden im Folgenden beschrieben.

3.8 Vermittlungsstellen

Im vorangegangenen Kapitel wurden die Schwachstellen in den Endgeräten und die sich daraus ergebenden Probleme behandelt. Auf diese hat der Benutzer noch gewissen Einfluß, denn er wählt die Endgeräte aus einer breiten Angebotspalette auf dem freien Markt aus. Bei Telefonanlagen ist die Wahl schon etwas eingeschränkt: Die meisten - insbesondere die größeren - TK-Anlagen funktionieren nur mit den dazugehörigen Endgeräten desselben Herstellers, weil sie proprietäre Protokollerweiterungen nutzen. Aber zumindest den Hersteller kann sich der Benutzer nach ihm wichtigen Kriterien aussuchen. Gar keinen Einfluß hat er bei den Vermittlungsstellen, an die die Endgeräte angeschlossen werden. Im Bereich der Deutschen Telekom gibt es nur zwei Typen von Teilnehmervermittlungstellen: Die EWSD von Siemens und die S12 von SEL-Alcatel.

An welche ein Benutzer angeschlossen wird, bestimmt sein Wohn- bzw. Standort und nicht sein Wunsch.

3.8.1 Die Vermittlungssoftware

Die Software für die Vermittlungsstellen wird salopp als „Dinosaurier“ bezeichnet, zum einen wegen ihres Alters und zum anderen wegen ihrer Größe.

Die Software ist in ihren Grundzügen schon sehr alt und wurde über die Jahrzehnte kontinuierlich weiterentwickelt und an neue Anforderungen angepaßt. Einmal jährlich wird eine neue Softwareversion freigegeben. Die Grundlage der heutigen Vermittlungssoftware stammt zum Teil noch aus den sechziger Jahren.

Zum anderen ist sie mit vielen Millionen Zeilen Code so groß, daß sie kein einzelner Mensch mehr verstehen kann. Das bringt Probleme mit sich:

Niemand weiß genau, ob die Software fehlerfrei ist. Man kann davon ausgehen, daß sie es also nicht ist. In jedem Update sind zwar alte Fehler beseitigt, da aber gleichzeitig neue Funktionen hinzukommen, können sich auch neue Fehler einschleichen. Aber es weiß auch niemand, wann und wo ein Fehler auftreten wird und wozu dieser führt.

Mir wurde zum Beispiel berichtet, daß jemand Anfang 1997 unbeabsichtigt ein Telefongespräch einer Firma mitgehört hat, weil ihn die Vermittlungsstelle offensichtlich fälschlich auf den selben Ferngesprächskanal geschaltet hat. Man stelle sich einmal vor was passiert, wenn Kriminelle diesen Fehler gezielt reproduzieren und sich auf jede beliebige Verbindung aufschalten können.

Deshalb wäre es notwendig, die komplette Vermittlungssoftware von Grund auf mit modernen Methoden des Software-Engineerings neu zu entwickeln. Nur so besteht die Chance, sie komplett zu durchschauen und Sicherheitslücken im Design zu erkennen, bevor sie von Hackern aufgedeckt und ausgenutzt werden. Doch vor den immensen Kosten der Neuentwicklung scheuen sich die Verantwortlichen.

3.8.2 Das Testzentrum der Telekom in Nürnberg

Das Technologiezentrum der Deutschen Telekom unterhält in Nürnberg eine Außenstelle. Dort existiert ein kleines Abbild der Telekommunikationswelt: Von beiden in Deutschland verwendeten Vermittlungsstellentypen existiert jeweils eine Auslands-, eine Fern- und zwei Ortsvermittlungsstellen. Sie alle sind untereinander so vernetzt wie im tatsächlichen Telefonnetz. Jeweils ein Teil von ihnen läuft unter der aktuellen Softwareversion, der Rest mit der Vorgängerversion. So kann man auch das Zusammenwirken der verschiedenen Softwareversionen der beiden Hersteller testen. Das ist notwendig, weil die Software nicht in allen Vermittlungsstellen gleichzeitig ausgetauscht werden kann, so daß auch im tatsächlichen Betrieb verschiedene Versionen zusammenarbeiten müssen.

In einem Testlabor stehen den D-Kanal-Spezialisten etwa hundert Telefonapparate zur Verfügung. Darunter befinden sich sowohl digitale als auch analoge Endgeräte, die zum Teil an TK-Anlagen und zum Teil direkt angeschlossen sind. Die verwendeten TK-Anlagen verfügen sowohl über Basis- als auch über Primärmultiplexanschlüsse. Über zwei Rechner haben die Tester Zugriff auf die Konfiguration der Testvermittlungsstellen. Sie können die Berechtigungen ihrer Telefonanschlüsse verwalten und ihr Verhalten testen. Um den Ablauf im D-Kanal zu beobachten, verfügen sie über Meßplätze mit Analysesoftware, die jedes Byte im D-Kanal aufzeichnen und in Klartext übersetzen kann. Mit Hilfe der ETSI⁵⁴-Spezifikationen werden neue Softwareversionen und neue Dienstmerkmale ausgiebig getestet, bevor sie in den öffentlichen Vermittlungsstellen zum Einsatz kommen. Mittels Protokollsimulatoren lassen sich auch unsinnige und unzulässige Nachrichten testen, wie sie manipulierte oder defekte Endgeräte verschicken könnten.

Damit können in Nürnberg sehr viele Konfiguration des realen Telefonnetzes nachgebildet und untersucht werden.

3.9 Schwachstellen in /Angriffe auf Vermittlungsstellen

3.9.1 Eindringen in die Vermittlungsstelle

In eine Vermittlungsstelle kann man auf verschiedene Weisen eindringen: Die klassische Möglichkeit ist der Einbruch in die Räume, in denen sich die Hardware befindet. Daneben kann man aber auch aus der Ferne über eine der Leitungen eindringen und Manipulationen an der Software und der Anlagenkonfiguration vornehmen.

Nach einem erfolgreichen Einbruch in die Vermittlungsstellen kann der Angreifer physikalisch an den Anschlüssen und der Hardware manipulieren. Er kann beispielsweise eine Teilnehmerbaugruppe gegen eine manipulierte austauschen, Filter außer Betrieb setzen, an der Vermittlungsstellensoftware manipulieren oder Anschlüsse umkonfigurieren.

Nach offiziellen Aussagen der Telekom sind alle Vermittlungsstellen nach Außen hin abgesichert. Nur wer eine gültige Chipkarte hat, kann sie auf normalem Wege betreten.

⁵⁴ ETSI = „European telecommunication standards institute“ mit Sitz in Frankreich

Und jedes Eindringen, mit oder ohne Berechtigung, wird protokolliert. Gegebenenfalls wird in einer übergeordneten Stelle Alarm ausgelöst.

Zusätzlich wird jeder autorisierte Programmiervorgang zusammen mit der Benutzererkennung protokolliert und ist so nachvollziehbar.

Von jedem ISDN-Anschluß aus lassen sich mit Hilfe einer ISDN-Karte beliebige Pakete auf dem D-Kanal an die Vermittlungsstelle schicken. Damit kann man versuchen, diese in einen undefinierten Zustand zu bringen.

Doch die Vermittlungsstellensoftware prüft jedes eingehende Paket auf Gültigkeit.

Man muß also eine Lücke in der Gültigkeitsprüfung finden, die es einem noch dazu erlaubt, gezielt eine Aktion in der Vermittlungsstelle auszulösen oder diese zu veranlassen, einen Teilnehmer zu manipulieren. Denn es gibt keinen durchgehenden D-Kanal von einem Teilnehmer zum anderen.

Jede Vermittlungsstelle verfügt über Wartungszugänge. Dabei muß man unterscheiden zwischen Prüf- und Administrationszugängen:

Über einen Prüfzugang wählt sich ein Techniker ein, der bei einem Teilnehmer oder an einem Verteilerkasten mit dem Entstören eines Anschlusses beauftragt ist. Aussagen des Chaos Computer Clubs zufolge kann man sich über das Telefonnetz in den Prüfzugang einer anderen Vermittlungsstelle einwählen und für andere Teilnehmer eine solche Prüfung veranlassen. Wenn diese gerade telefonieren, wird ihre Verbindung getrennt, andernfalls werden sie von der Vermittlungsstelle angerufen. Der auslösende Anrufer kann damit kostenlos andere Telefonteilnehmer belästigen.

Nach Aussagen der Hackervereinigung „The Hacker’s Choice“⁵⁵ gibt es einen weiteren Zugang für Techniker⁵⁶. Dieser ist auch in anderen Ortsnetzen zu erreichen und bietet umfassendere Prüfmöglichkeiten, unter anderem auch das Aufschalten auf beliebige Verbindungen. Anders als der oben beschriebene Zugang ist dieser mit zwei vierstelligen Zahlen als Benutzererkennung und Passwort abgesichert.

Über den Administrationszugang einer Vermittlungsstelle wird diese selbst ferngesteuert. Vermittlungsstellen verfügen zwar immer auch über einen eigenen Administrationsrechner, der wird aber in den seltensten Fällen genutzt, denn sie arbeiten normalerweise unbemannt. Aus zentralen Wartungszentren können Telekom-Techniker neue Software in die Vermittlungsstelle einspielen und die Konfiguration der gesamten Anlage oder einzelner Anschlüsse verändern.

Wenn es einem Angreifer gelingt, sich in eine solche Verbindung einzuschalten, kann er mit der Vermittlungsstelle machen was er will. Wenn es ihm zusätzlich gelingt, manipulierte Software einzuspielen, kann er sich auch Hintertürchen für weitere Angriffe schaffen. Diese können dann beispielsweise über den D-Kanal erfolgen, indem er undefinierte Pakete schickt, auf die die von ihm manipulierte Software reagiert.

Der Netzbetreiber versucht sich dagegen abzusichern, indem er alle Zugriffe auf eine Vermittlungsstelle mit einer Login-Prozedur absichert und alle Veränderungen an der Konfiguration protokolliert.

Darüber hinaus soll in Zukunft der Zugriff nur noch nach Authentisierung durch eine Chipkarte möglich sein.

⁵⁵ siehe [thc97]

⁵⁶ SEPT (System-Externe-Prüf-Technik)

Ein Angreifer kann versuchen, an die Quelltexte der Vermittlungsstellensoftware der beiden Hersteller Siemens und SEL Alcatel heranzukommen, um sie zu manipulieren. Das ist aufgrund der Größe der Software allerdings für einen einzelnen Angreifer sehr schwierig.⁵⁷

Alternativ kann er sich Verbündete bei den Herstellerfirmen suchen, die die gewünschten Manipulationen in die nächste Softwareversion einpflanzen. Gerade wegen der Unüberschaubarkeit haben sie gute Chancen, nicht entdeckt zu werden.

Damit lassen sich undefinierte Paket-Typen einführen, die im Normalfall nicht auftreten. Der Angreifer kann dann gezielt solche Pakete zu seiner Vermittlungsstelle schicken, und sie damit veranlassen, für ihn zu arbeiten.

3.9.2 Gefahrenpotential von Centrex-Teilnehmern

In den USA ist dieser Service schon lange erfolgreich, langsam setzt er sich auch in Deutschland durch: Centrex. Das Akronym steht für „Central Exchange“ und wird im Deutschen gerne als „virtuelle Nebenstellenanlage“ umschrieben.

Damit kann beispielsweise ein Unternehmen mit verschiedenen Standorten eine unternehmensweite Telefonanlage aufbauen, ohne wirklich eine Anlage zu besitzen. Alle Telefone erhalten zwei Rufnummern: Eine normale Nummer mit Vorwahl und eine Nebenstellenummer ohne Vorwahl. Über die normale Nummer können sie von jedem Telefonanschluß weltweit erreicht werden. Über die Nebenstellenummer können sie von allen Anschlüssen innerhalb ihrer Centrex-Gruppe erreicht werden. Die Gespräche innerhalb der Gruppe sind kostenlos, die anderen Gespräche werden zu normalen Tarifen berechnet. Außerdem stehen Leistungsmerkmale wie Heranholen des Rufes, automatischer Rückruf etc. innerhalb der Gruppe zur Verfügung. Eine solche Centrex-Gruppe verhält sich also wie eine TK-Anlage, die Gesprächssteuerung wird aber über die Vermittlungsstellen abgewickelt.

Damit der Kunde die Rechte der Teilnehmer in seiner Centrex-Gruppe selbst verwalten kann, muß es einen speziellen Operator-Platz geben: Das ist ein PC mit einer ISDN-Karte und spezieller Software, über die sich der Operator bei seiner Vermittlungsstelle anmeldet. Dann kann er über das Netz der Vermittlungsstellen alle Teilnehmer seiner Centrex-Gruppe verwalten. Die Kommunikation geschieht über das D-Kanal-Protokoll, das um entsprechende Merkmale erweitert werden muß.

Daraus ergeben sich zwei mögliche Angriffsstellen: Angriffe *durch* Centrex-Teilnehmer und Angriffe *auf* sie:

Ein Centrex-Operator hat einen gewissen Zugriff auf seine Vermittlungsstelle, der über den normalen Zugriff über den D-Kanal hinausgeht. Er hat das Recht, den anderen Anschlüssen in der von ihm verwalteten Centrex-Gruppe Berechtigungen zuzuweisen oder zu entziehen. Dieses Recht könnte er durch einen geeigneten Angriff auch auf normale Telefonanschlüsse außerhalb seiner Centrex-Gruppe oder auf andere Gruppen ausdehnen und sie so manipulieren.

Andererseits müssen die Berechtigungen aller Centrex-Teilnehmer durch ihren Operator aus der Ferne veränderbar sein. Daraus ergibt sich die Gefahr, daß diese Anschlüsse auch von Anderen manipulierbar sein könnten.

⁵⁷ siehe Abschnitt 3.8.1

Doch darüber kann man erst dann Näheres sagen, wenn Centrex in Deutschland fertig eingeführt ist. Damit kann man rechnen, sobald die Hersteller der Vermittlungsstellen ihre Software dafür fertiggestellt haben.

3.9.3 Umkonfigurieren von Anschlüssen

Wenn es einem Angreifer gelingt, eine Vermittlungsstelle zu manipulieren, so daß er an die Konfiguration seines oder anderer Anschlüsse herankommt, kann er Rufumleitungen an anderen Anschlüssen einrichten, CLIP fest aktivieren oder den eigenen Anschluß zu einem Notruf- oder einem Katastrophenanschluß machen:

Ein Angreifer könnte an einem Anschluß im selben Ortsnetz eine Rufumleitung ins Ausland einrichten und dann zum Ortstarif dorthin telefonieren. Die teuren Auslandsgebühren bezahlt der Manipulierte.

Alternativ könnte er auch eine Rufumleitung zu einer 0190-Nummer einrichten und dann ständig den manipulierten Anschluß anwählen. Damit kann er nicht nur kostenlos telefonieren sondern selbst Geld verdienen.⁵⁸

Kostenlos für den Betroffenen ist es, wenn ein Angreifer an dessen Anschluß die Rufnummernübermittlung (CLIP) fest einschaltet. Wo immer er dann anruft, wird seine Rufnummer zu sehen sein, auch wenn er das gar nicht möchte. Dieser Angriff ist eher datenschutzrechtlich relevant.

Interessanter für den Angreifer ist es, seinem eigenen Anschluß besondere Rechte einzuräumen. Im Netz der Telekom gibt es zwei besondere Typen von Anschlüssen: den Katastrophenanschluß und den Notrufanschluß:

Der Katastrophenanschluß ist ein bevorrechtigter Anschluß. Wenn eine Ortsvermittlungsstelle überlastet ist, werden die Katastrophenanschlüsse zuletzt abgeschaltet. Solche Anschlüsse werden Ärzten, Apotheken, Hilfsorganisationen, der Polizei und den Feuerwehren zugeteilt, damit diese auch im Falle einer Überlastung des Ortsnetzes noch immer telefonieren können. Daran könnte auch ein Angreifer interessiert sein, wenn er gezielt ein Ortsnetz überlastet, um Andere am Telefonieren zu hindern, selbst aber noch telefonieren will.

Der Notrufanschluß hat die sogenannte „overwrite“-Berechtigung. Wenn ein Anrufer einen solchen Anschluß wählt, wird dort immer seine Rufnummer angezeigt. Auch dann, wenn er dies ausdrücklich unterbinden will⁵⁹ oder noch einen analogen T-Net-Anschluß besitzt. Die overwrite-Berechtigung wird nur Notrufabfrageplätzen der Polizei, der Feuerwehr und des Rettungsdienstes zugewiesen. Doch auch Andere haben ein Interesse daran, immer zu sehen, wer sie anruft. Da der Anrufer das nicht erkennen kann, entsteht auch hier ein datenschutzrechtliches Problem.

3.9.4 Abhören von Gesprächen/Räumen

Wenn es einem Angreifer gelingt, eine Vermittlungsstelle in seine Gewalt zu bringen, kann er sie dazu veranlassen, D-Kanal-Pakete an einen anderen Anschluß zu schicken. Damit kann er möglicherweise Räume oder Gespräche an diesem Anschluß abhören. Ihm stehen dabei etwa die selben Möglichkeiten zur Verfügung wie beim Eindringen in eine

⁵⁸ siehe Abschnitt 3.9.8

⁵⁹ CLIR = Calling Line Identification Restriction

TK-Anlage.⁶⁰ Sogar dann, wenn der Angegriffene eine gut abgesicherte oder gar keine TK-Anlage betreibt.

Er kann sich auch direkt in der Vermittlungsstelle auf eine Verbindung seiner Wahl aufschalten und sie abhören oder manipulieren.

3.9.5 Kostenloses Telefonieren

3.9.5.1 Blueboxing

Im analogen Netz mit digitalisierten Vermittlungsstellen wird die Zeichengabe zwischen den Vermittlungsstellen über Töne durchgeführt. Dabei kommen ähnliche Töne zum Einsatz wie die, die Telefone im Mehrfrequenzwahlverfahren (MFV) erzeugen. Mit Hilfe eines manipulierten MFV-Senders, einer sogenannten „blue-box“ kann man diese Töne selbst erzeugen und damit Vermittlungsstellen manipulieren. Blue boxes wurden in großem Umfang in den USA,⁶¹ später auch in Deutschland eingesetzt, um kostenlos zu telefonieren.⁶²

Das geht im ISDN so nicht mehr, weil die Vermittlungsstellen untereinander nicht mehr über Tonsignale kommunizieren und weil die gesamte Signalisierung außerhalb des Sprachkanals stattfindet.⁶³

3.9.5.2 Über die Telefonanlagen von Firmen

Nahezu alle großen Firmen verfügen heute schon über eine ISDN-Anlage. Häufig ist diese auch mit einem Voice-mail-system verknüpft. Diese moderne Form des Anrufbeantworters speichert eingehende Nachrichten in einem zentralen Rechner und stellt sie dem berechtigten Benutzer zum Abruf bereit. Ob ein Benutzer berechtigt ist, entscheidet die Anlage nach Eingabe eines Passworts. Oftmals kann ein Benutzer über ein Voice-mail-system auch eine Amtsleitung bekommen, um darüber auf Firmenkosten zu telefonieren. Insbesondere bei Außendienstmitarbeitern wird diese Möglichkeit gerne genutzt. Sie wählen sich über eine kostenlose Rufnummer in die Telefonanlage ihrer Firma hinein und können dann auf Firmenkosten ihren Gesprächspartner anrufen.

Wenn es einem Angreifer gelingt, den Code eines Mitarbeiters herauszufinden, kann er ebenfalls auf diese Weise auf Firmenkosten telefonieren.⁶⁴

3.9.5.3 Abschalten der Gebührenerfassung

Die Gebühren werden im ISDN auf zwei voneinander unabhängige Weisen erfaßt. Zum einen erhält der rufende Teilnehmer während⁶⁵ oder am Ende⁶⁶ eines Gesprächs Gebühreninformationen über den D-Kanal zugeschickt. Diese dienen aber nur der Information des Teilnehmers und sind nicht rechtsverbindlich.⁶⁷ Diese zu manipulieren oder abzuschalten spart also keine Gebühren.

⁶⁰ vgl. Kapitel 2

⁶¹ vgl. [hau96]

⁶² vgl. z.B. Chip 2/94, Focus 6/94

⁶³ outband signalling, siehe Abschnitt 3.3

⁶⁴ vgl. [hau96]

⁶⁵ AOCD = Advice Of Charge During a call

⁶⁶ AOCE = Advice Of Charge at the End of a call

⁶⁷ sehr umstritten. Die Telekom erkennt nur ihre eigene Zählung an

Zum anderen werden in der Vermittlungsstelle des Anrufers Datum, Anfangszeit, Dauer und Zielrufnummer⁶⁸ eines Gesprächs gespeichert. Diese werden in der sogenannten „Nachbearbeitung“ durch ein anderes Softwarepaket ausgewertet und dem Teilnehmer in Rechnung gestellt. Die Speicherfunktion ist in der Vermittlungsstellen-Software enthalten und nach offiziellen Aussagen nicht programmgesteuert abschaltbar. Ein Angreifer muß also eine manipulierte Vermittlungsstellensoftware einspielen.⁶⁹

3.9.6 Denial of Service durch Prüfschleifen

Jeder ISDN-Anschluß verfügt über sogenannte Prüfschleifen. Aus der Vermittlungsstelle heraus kann ein Servicetechniker zu Prüfzwecken folgende Netzbestandteile in den Schleifenzustand versetzen:

- die Vermittlungsstelle,
- einen eventuell vorhandenen Zwischenregenerator (ZWR) bei langen Leitungen
- den NT beim Benutzer
- die Terminaladapter (TA) und Endeinrichtungen (TE) beim Benutzer

Sie senden dann alle empfangenen Bits zurück an den Absender. So entstehen die sogenannten Prüfschleifen, mit deren Hilfe sich ein Fehler eingrenzen läßt.

Ein Angreifer, der Zugriff auf den Prüfschleifenmechanismus hat, kann einen beliebigen Anschluß an der Vermittlungsstelle außer Betrieb nehmen („denial of service“), indem er eine Prüfschleife aktiviert. Der Anschlußinhaber kann dann nicht mehr telefonieren.

3.9.7 Kostenlose Datenübertragung im D-Kanal

Gemäß ETSI-Spezifikation gibt es drei Möglichkeiten, über den D-Kanal kurze Nachrichten zwischen zwei Endgeräten auszutauschen (User-to-User-Signalling (UUS)). Im Netz der Telekom wird jedoch nur die Variante UUS-1 angeboten. Die Variante 2 ist nicht implementiert. Bei der Variante 3 können die Endgeräte während einer bestehenden Verbindung kurze Datenpakete austauschen. Sie ist zwar in der Vermittlungsstellensoftware implementiert, wird aber von der Telekom nicht angeboten.

User-To-User-Signalling 1 dient dem Austausch einer maximal 32 Byte langen Nachricht schon während des Verbindungsaufbaus. Damit kann der eine Benutzer dem anderen einen kurzen Text zusammen mit seiner Telefonnummer auf das Display schicken, ohne daß eine Verbindung aufgebaut werden muß. Für diese Nachricht entstehen auch keine Gebühren.

Findige Hardwarehersteller haben relativ schnell spezielle ISDN-Karten entwickelt, die kostenlos auch größere Datenmengen über das Telefonnetz übertragen können: Die Daten werden in 32-Byte-Blöcke segmentiert, die Zielrufnummer immer wieder angewählt und jeweils ein Block übertragen. Dann wird der Verbindungsaufbau abgebrochen und mit dem nächsten Block neu eingeleitet. Um die Geschwindigkeit noch zu erhöhen, weist die angerufene Karte das Gespräch ab, sobald sie die Daten empfangen hat. Ein Verbindungsaufbau dauert maximal 1,7 Sekunden, typisch sind etwa 1 Sekunde. Damit läßt sich eine mittlere Datenübertragungsrate von 32 Bytes/sec erreichen - kostenlos und zu jedem beliebigen ISDN-Anschluß in Deutschland.

Der Anschluß der beteiligten Teilnehmer bleibt auch weiterhin nutzbar, weil keine B-Kanäle für die Datenübertragung verwendet werden.

⁶⁸ verkürzt um die letzten drei Stellen

⁶⁹ siehe Abschnitt 3.9.1

Diese Vorgehensweise entspricht aber nicht der vertragsgemäßen Verwendung des Telefonanschlusses und die Telekom versucht sich dagegen zu wehren. Dafür werden spezielle Steuerkanal-Überwachungen eingesetzt.⁷⁰

3.9.8 Das Geschäft mit den 0190-Nummern

In den Jahren 1994/95 meldeten viele Zeitungen immer wieder Mißbrauch von 0190-Rufnummern zum Gebührenbetrug.

Der Inhaber einer Service-0190-Rufnummer kassiert, wenn jemand seinen Service anruft. Der Anrufer bezahlte damals⁷¹ über seine Telefonrechnung 1,15 DM an die Telekom, die zweigte davon 55 Pfennig ab und zahlte sie an den Betreiber.

Betrüger fanden verschiedene Wege, die Zahl der Anrufminuten für ihre Servicenummern in die Höhe zu treiben. Dazu gehören der Einsatz von Auto-Dialern, Rufumleitungen an fremden Anschlüssen und unbenutzte Teilnehmeranschlüsse:

Ein Auto-Dialer ist ein automatisches Wählgerät im Zigarettenschachtel-Format. Es kann bei Aktivierung vollautomatisch eine vorher eingestellte Telefonnummer anwählen. Normalerweise werden Auto-Dialer zum Beispiel in Alarmanlagen benutzt, um bei Alarmauslösung Hilfe herbeizurufen. Doch die Geräte lassen sich in Telefonnetzen mit „in-band“-Signalisierung auch mißbrauchen:

Kriminelle richten einen Servicedienst ein und lassen ihn mittels Auto-Dialern manchmal nächtelang ununterbrochen anwählen. Dazu mußten sie nur den unauffälligen Auto-Dialer irgendwo an der Leitung zwischen Kunde und Vermittlungsstelle anbringen.

Im ISDN benötigt man für einen solchen Angriff aufwendigere und deshalb teurere Technik. Sie muß in der Lage sein, sich auf die Leitung aufzuschalten, die beiden B-Kanäle vom D-Kanal zu trennen und über den D-Kanal Wahlbefehle mit den richtigen Parametern an die Vermittlungsstelle zu schicken. Mit einem einfachen Auto-Dialer für 100,- Mark aus dem Katalog ist es da nicht getan.

Wenn es einem Angreifer gelingt, an einem Anschluß eine Rufumleitung zu seinem 0190-Service zu aktivieren, muß er nur noch den manipulierten Anschluß anwählen und er wird automatisch weiterverbunden. Für ihn entstehen nur die normalen Telefonkosten - im besten Fall zum Ortstarif.

Von den Gefahren bei der Rufumleitung sind nicht nur ISDN-Anschlüsse sondern in noch größerem Umfang auch die ANIS-Teilnehmer betroffen. Das sind Teilnehmer mit analogen Anschlüssen an digitalen Vermittlungsstellen⁷². Sie können gegen Aufpreis einige Leitungsmerkmale aus dem ISDN bekommen, darunter auch die Rufumleitung. Um eine Rufumleitung einzurichten, zu aktivieren oder zu deaktivieren, muß der Teilnehmer eine Verbindung mit der Vermittlungsstelle aufbauen⁷³. Er tippt dann den Aktivierungscode, seine PIN und gegebenenfalls die Zielrufnummer ein. Standardmäßig ist die PIN „0000“ und nach Aussagen von Insidern haben bis heute 70% der Nutzer der Rufumleitung ihre PIN nicht geändert. Ein Angreifer kann sich auf die Leitung aufschalten und eine Rufumleitung einrichten.

⁷⁰ siehe Abschnitt 5.2.2

⁷¹ Heute gibt es verschiedene Tarife bis 3,20 DM pro Minute. Das Prinzip ist aber gleichgeblieben.

⁷² Ende 1997 sollen alle Anschlüsse entweder ISDN oder ANIS sein.

⁷³ Das heißt insbesondere, er muß den Hörer abheben.

1994 wurden mehrere Betrugsfälle aufgedeckt, bei denen die Betreiber der Service-Nummern Komplizen bei der Telekom hatten. Diese haben Auto-Dialer auf nicht benutzte Ports in den Vermittlungsstellen geschaltet. Dadurch entstanden Gebühren, die die Telekom an die Betreiber abführen mußte, ohne jedoch selbst Einnahmen zu haben.

3.9.9 Manipulation anderer Vermittlungsstellen

Wenn es einem Angreifer erst einmal gelungen ist, eine Vermittlungsstelle in seine Gewalt zu bekommen, kann er von dort aus das gesamte restliche Netz angreifen: Die Vermittlungsstellen sind untereinander über ein eigenes Zeichengabernetz verbunden, das sogenannte Zeichengabesystem-7 (ZGS7). Jede Vermittlungsstelle stellt einen Knoten in diesem Netz dar und hat eine netzweit eindeutige Adresse. Über das Netz können sich die Vermittlungsstellen Nachrichten zusenden, die der Steuerung von Nutzkanalverbindungen dienen. Das kann ein Angreifer auch mißbrauchen, um einen Fernangriff durchzuführen. Das nächste Kapitel ist der Sicherheit im Zeichengabesystem 7 gewidmet.

4 Das Zeichengabesystem 7

4.1 Einleitung

Dieses Kapitel beschäftigt sich mit der Sicherheit in den oberen Ebenen der Telekommunikationsnetze. Nachdem in den beiden vorangegangenen Kapiteln die Sicherheit der Endgeräte und der Vermittlungsstellen betrachtet wurde, steht jetzt das Netzwerk zwischen den Vermittlungsstellen im Vordergrund. Dieses Netzwerk erstreckt sich von den Teilnehmervermittlungsstellen in der Ortsebene über mehrere Hierarchiestufen bis hin zum weltumspannenden internationalen Zeichengabesystem. Große Teile davon werden mit dem CCITT-Zeichengabesystem 7 betrieben.

4.2 Zeichengabesysteme

Zur Steuerung der Telekommunikationsnetze benötigt man die Möglichkeit, Informationen parallel zu den eigentlichen Nutzdaten der Verbindungen zu übertragen. Dazu gibt es prinzipiell zwei Möglichkeiten: Signalisierung im Sprachkanal und in einem eigenen Steuerkanal.

4.2.1 Im-Band-Signalisierung⁷⁴

Früher verwendete man zur Steuerung die sogenannte Im-Band-Signalisierung: Auf die übertragene Sprache wird die Steuerinformation aufmoduliert und im selben Kanal übertragen. Auch heute noch funktionieren einige nationale analoge Netze nach diesem Prinzip. Darunter auch das analoge Netz der Telekom. Hier kommen Impuls- und Mehrfrequenzzeichengabe zum Einsatz:

Bei den noch nicht digitalisierten Ortsvermittlungsstellen im Netz der Telekom wird das Impulszeichengabesystem verwendet.

Für jede zu wählende Ziffer wird eine entsprechende Anzahl Unterbrechungen auf der Telefonleitung erzeugt. Es gibt nur die Ziffern 0-9. Die Sonderwählzeichen * und # können nicht dargestellt werden.

Auch die bereits digitalisierten Ortsvermittlungsstellen verstehen die Impulszeichengabe noch, damit die Kunden ihre alten Endgeräte weiterverwenden können. Neue Endgeräte sind aber immer für Mehrfrequenzzeichengabe ausgerüstet.

Bis Ende 1997 werden alle Ortsvermittlungsstellen in Deutschland digitalisiert sein.

Die Mehrfrequenzzeichengabe wird in Deutschland erst seit Beginn der Digitalisierung des Telekommunikationsnetzes verwendet. Sie kommt bei analogen Anschlüssen an digitalen Vermittlungsstellen⁷⁵ zum Einsatz

In den USA wird dieses Verfahren schon länger verwendet. Die Endgeräte erzeugen für jede zu wählende Ziffer einen Ton, der aus zwei verschiedenen Frequenzen zusammengesetzt wird. Der Teilnehmer kann an seinem Endgerät Töne für die Ziffern 0-9 und die Sonderziffern * und # erzeugen und so Verbindungen zu anderen Teilnehmern aufbauen und steuern.

⁷⁴ inband-signalling

⁷⁵ sog. ANIS-Teilnehmer

Mit anderen Frequenzen, aber nach dem selben Prinzip wurde in den USA auch die Steuerung der Vermittlungsstellen durchgeführt. Inzwischen wird dort auch das Zeichengabesystem 7 eingesetzt.

4.2.2 Das Problem des Blueboxing

Hacker haben schnell herausgefunden, daß sie die passenden Töne zur Steuerung des Netzes auch selbst erzeugen und damit kostenlos telefonieren können: Sie wählten eine kostenlose Telefonnummer, signalisierten dem Netz, sie hätten aufgelegt und ließen sich von der überlisteten Vermittlungsstelle zu einem Gesprächspartner ihrer Wahl verbinden. Nach der Farbe des ersten dafür gebauten Geräts nennt man diese Art des Gebührenbetrugs auch Blueboxing.

Die Telefongesellschaften reagierten auf den Betrug zunächst, indem sie regelmäßig die verwendeten Frequenzen wechselten. Doch die Hacker waren schneller. Sie hatten die neuen Codes meist schon vor dem Inkrafttreten von Mitarbeitern der Telefongesellschaften gekauft.

In einem zweiten Schritt wurde zusätzliche Hardware in den Vermittlungsstellen installiert, die die betrügerischen Töne filterte, wenn sie von einem Teilnehmer kamen. Zum Teil waren diese Filter aber genauer eingestellt, als die Auswerter für die Töne, die geschützt werden sollten: Die Hacker variierten die Frequenzen ein wenig und konnten weiter betrügen. Daraufhin wurden Geräte installiert, die ein breiteres Frequenzspektrum filtern konnten, indem sie Töne aus diesem Bereich etwas anhoben oder senkten, so daß sie außerhalb des erkannten Bereichs lagen. Doch auch das konnte Hacker nicht aufhalten: Sie sendeten Töne, die entsprechend zu hoch oder zu tief lagen. Diese wurden dann von den Filtern in die richtige Frequenz umgesetzt.

In Deutschland war blueboxing nie weit verbreitet. Die wenigen Blueboxer wählen sich über 0130-Nummern ausländischer Unternehmen in andere Netze und treiben dort ihr Unwesen.

4.2.3 Außer-Band-Signalisierung⁷⁶

Die richtige Lösung für das Problem des Blueboxing brachte erst der Umstieg auf die außer-Band-Signalisierung im Zusammenhang mit der Digitalisierung der Telekommunikationsnetze. Hier werden die Steuerinformationen über ein eigenes, von den Nutzverbindungen unabhängiges Netz übertragen. Damit stehen die Nutzkanäle voll transparent zur Verfügung: Die Kommunikationspartner können übertragen was sie wollen, sie werden damit nie das Netz an sich beeinflussen.

Ein weiterer Vorteil ist die Möglichkeit, Steuerungsinformationen auch unabhängig von einer Nutzkanal-Verbindung zu übertragen. Das wird vor allem bei intelligenten Netzen und bei Mobilfunknetzen genutzt.

Außerdem können bei Außer-Band-Signalisierung auch während einer aktiven Verbindung Steuerungsinformationen ausgetauscht werden, ohne die Verbindungsqualität zu beeinflussen.

Bei inband-Zeichengabe stört Übermittlung des Gebührenimpulses mit 16 kHz-Tönen beispielsweise die Datenübertragung mit Modems.

⁷⁶ outband signalling

Ein System, mit dem außer-Band-Signalisierung durchgeführt wird, ist das Zeichengabesystem 7. Auch der Vorgänger, Zeichengabesystem 6 arbeitete bereits auf diese Weise, wurde aber wegen verschiedener Mängel abgelöst.

4.3 Der Aufbau des CCITT Zeichengabesystems 7⁷⁷

In digitalen Telekommunikationsnetzen wird heute zunehmend das CCITT-Zeichengabesystem 7⁷⁸ zur Steuerung verwendet. Zahlreiche Netzbetreiber auf der ganzen Welt haben ein solches System bereits eingeführt oder planen die Einführung in naher Zukunft. Zwischen den Vermittlungsstellen innerhalb eines Netzes und zwischen verschiedenen Netzen existieren eigene Zeichengabe-7-Netzwerke, die die Steuerungsaufgaben wahrnehmen.

Im Folgenden werden das ZGS 7 und die damit aufgebauten Netze beschrieben, dann folgen Sicherheitsbetrachtungen.

Die ersten Teile des ZGS-7 sind bereits vor der Verabschiedung des ISO/OSI 7-Schichten-Modells veröffentlicht worden. Sie sind in vier Schichten gegliedert, die in ihren Aufgaben von denen des 7-Schichten-Modells abweichen. Bei später definierten Teilen des ZGS-7 wurde streng nach dem OSI-Modell vorgegangen.

Im Folgenden werden die für die ISDN-Netze wichtigsten Teile kurz beschrieben:

4.3.1 Der message-transfer-part MTP⁷⁹

Der Nachrichten-Transferteil (message-transfer-part, MTP) stellt eine Verbindung zwischen zwei benachbarten Zeichengabepunkten her und sorgt für eine ausfallsichere Übertragung der Steuerungsinformationen zwischen ihnen. Er übernimmt die Aufgaben der unteren drei Schichten des ZGS-7. Dazu gehören die physikalische Übertragung der Daten über den Kanal in Schicht 1, die Zeichengabestreckenfunktionen und Ausfallsicherungen in Schicht 2 und die Zeichengabenetzfunktionen mit routing⁸⁰ in Schicht 3.

Die Funktionen des MTP sind grundlegend für alle anderen Teile und müssen deshalb in jedem Knoten des ZGS-7-Netzwerks implementiert sein.

Auf den MTP werden in der Schicht 4 verschiedene Anwenderteile aufgesetzt. Sie stellen virtuelle Ende-zu-Ende-Beziehungen zwischen der Ursprungs- und der Zielvermittlungsstelle her und sind im Folgenden näher beschrieben:

4.3.2 Der ISDN-user-part ISUP⁸¹

Der ISDN-Anwenderteil (ISDN-user-part, ISUP) ist die Schnittstelle zwischen den Vermittlungsstellen und dem ZGS-7-Netz. Er wurde als hardwareunabhängige Schnittstelle zwischen ISDN-Vermittlungsstellen definiert. Dadurch können Vermittlungsstellen verschiedener Hersteller über ihn kommunizieren und Nutzkanalverbindungen zwischen je zwei benachbarten Vermittlungsstellen auf- und abbauen. Durch das Hintereinanderschalten mehrerer Verbindungsabschnitte werden Ende-zu-Ende Verbindungen von der Ursprungs- zur Zielvermittlungsstelle erzeugt. Der ISUP stellt damit die Unmittelbare

⁷⁷ vgl. [ban-95]

⁷⁸ ZGS-7, international als „signalling-system No. 7“ bezeichnet, abgekürzt „SS7“ oder „No. 7“

⁷⁹ vgl. [kah92] Abschnitte 4.5.3.1-4.5.3.3 und [ban95] Abschnitt 6.3

⁸⁰ siehe Abschnitt 4.4.2

⁸¹ vgl. [kah92] Abschnitt 4.9 und [ban95] Abschnitt 6.5

Verlängerung des D-Kanal-Protokolls über die Grenzen einer Vermittlungsstelle hinaus dar.

4.3.3 Der signalling-connection-control-part SCCP⁸²

Der Steuerteil für Zeichengabeverbindungen (signalling-connection-control-part, SCCP) nimmt eine besondere Rolle ein: Er baut selbst auf der Ebene 3 auf, stellt aber auch für andere Schicht-4-Teile besondere Funktionen der Schicht 3 bereit. Je nach Betrachtungsweise gehört er deshalb der Schicht 3 oder 4 an.

Über den SCCP werden die virtuellen Ende-zu-Ende-Verbindungen zwischen den Vermittlungsstellen auf- und abgebaut.

4.3.4 Der transaction-capability-application-part TCAP⁸³

Der Anwenderteil für Transaktions-Funktionen (transaction-capability-application-part, TCAP) dient dazu, nicht-Nutzkanal-bezogene Informationen über das Zeichengabesystem auszutauschen. Die Einrichtungen des Zeichengabesystems werden zunehmend dezentralisiert. Außerdem werden immer neue Dienste hinzugefügt. Um beides weiterhin verwalten zu können wurde ein Nutzkanal-unabhängiger Informationsaustausch nötig.

Mit Hilfe des TCAP können Funktionen intelligenter Netze bereitgestellt werden. Dazu gehören beispielsweise die Datenbanken für die Services 0130, 0180 und 0190. Sie sind nur wenige Male in replizierter Form im gesamten deutschen Netz vorhanden. Will ein Teilnehmer eine solche Nummer anwählen, so sendet die Ursprungsvermittlungsstelle mittels einer TCAP-Nachricht eine Anfrage an die zuständige Datenbank. Als Antwort erhält sie die tatsächliche Rufnummer des gewünschten Teilnehmers. Zu diesem wird dann auf dem üblichen Wege eine Nutzkanalverbindung aufgebaut.

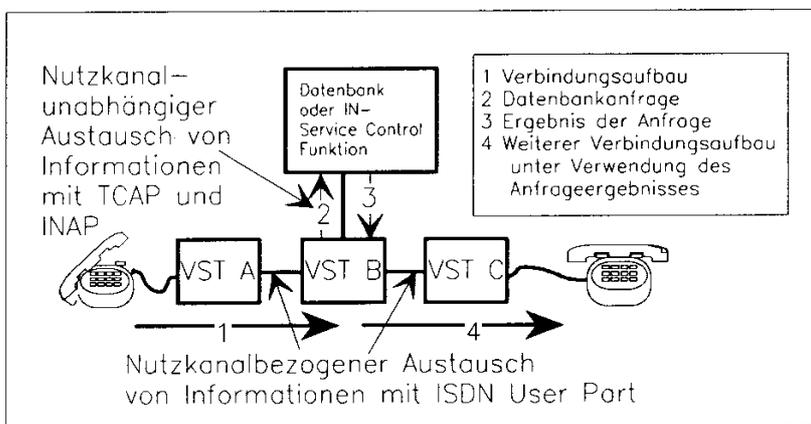


Abb. 6.77 — Informationsaustausch zwischen Datenbank und Vermittlungsstelle

aus [ban95] Seite 177

⁸² vgl. [ban95] Abschnitt 6.6

⁸³ vgl. [ban95] Abschnitt 6.7

4.3.5 Der operations-maintenance-and-administration-part OMAP⁸⁴

Der Anwenderteil für Bedienen und Unterhalten (operations-maintenance-and-administration-part, OMAP) stellt Funktionen für die Steuerung des Netzes selbst bereit. Diese Funktionen dienen nicht dem Auf- und Abbau von Nutzkanälen, sondern sollen ausschließlich die Funktionsfähigkeit des Zeichengabernetzes sicherstellen.

Management-Funktionen des TMN⁸⁵ sind sowohl Funktionen zur Steuerung der Vermittlungsstellen als auch solche zur Steuerung des ganzen Netzes. Zu den Funktionen zur Steuerung der Vermittlungsstellen gehören zum Beispiel das Einrichten und Verwalten von Teilnehmern. Zu den Netzsteuerungs-Funktionen gehört das Verkehrsmanagement. Hinzu kommen Funktionen zur Verwaltung der routing-Tabellen in den Zeichengabepunkten.⁸⁶

Das Folgende Bild⁸⁷ verdeutlicht die Zusammenhänge. Links stehen die Schichten des ISO/OSI-7-Schichten-Modells und rechts die Ebenen des Zeichengabesystems 7.

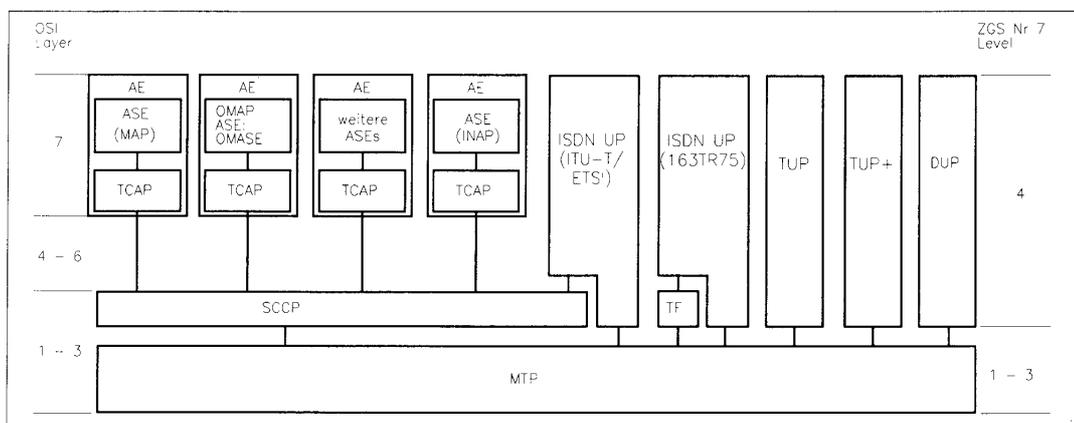


Abb. 6.2 — Derzeitige Komponenten des Zeichengabesystems Nr. 7

4.4 Zeichengabe-7-Netzwerke

4.4.1 Aufbau und Bestandteile

Ein ZGS-7 Netzwerk besteht im wesentlichen aus drei Komponenten: Zeichengabe-Endpunkten, Zeichengabe-Transferpunkten und Zeichengabestrecken.

Zeichengabe-Endpunkte⁸⁸ sind die Einrichtungen im Netz, von denen eine Zeichengabebeziehung ausgeht oder bei denen sie endet. Das können neben Vermittlungsstellen auch Datenbanken für Mobilfunk- oder intelligente Netze sein.

Zeichengabe-Transferpunkte⁸⁹ sind die Einrichtungen im Netz, die der Verbindung der beiden Zeichengabe-Endpunkte einer Zeichengabebeziehung dienen. Sie werten ankommende Informationen nicht aus sondern leiten sie auf dem Weg zum Empfänger an den

⁸⁴ vgl. [ban95] Abschnitt 6.9

⁸⁵ TMN = telecommunications management network

⁸⁶ siehe Abschnitt 4.4.2, Kapazität des Zeichengabernetzes

⁸⁷ aus [ban95], Seite 105

⁸⁸ signalling-endpoints, SEP

⁸⁹ signalling-transfer-points, STP

nächsten Zeichengabe-Punkt weiter. Sie übernehmen also die Aufgabe der Router des Netzwerks.

Zeichengabestrecken sind die Verbindungen zwischen Zeichengabe-Punkten.

Ein Zeichengabenetz wird so aufgebaut, daß von jedem Zeichengabe-Endpunkt jeder andere Zeichengabe-Endpunkt zu erreichen ist. Je mehr verschiedene Wege es dabei gibt, desto besser ist das Netz gegen Ausfälle geschützt. Wichtige Einrichtungen wie zum Beispiel Flughäfen können immer über verschiedene Leitungswege erreicht werden. Beim Ausfall des Hauptweges kann zumindest ein Notbetrieb über einen Ersatzweg aufrecht erhalten werden.

4.4.2 Kapazität des Zeichengabernetzes

Ein großer Nachteil der Nutzkanal-abhängigen Zeichengabe im herkömmlichen Telefonnetz ist die schlechte Netzauslastung. Hier wird vor und nach der eigentlichen Nutzverbindung ein Ende-zu-Ende-Kanal für die Zeichengabe benötigt. Da es nur Nutzkanäle einheitlicher Kapazität gibt, müssen diese dafür verwendet werden. In der Verbindungsauf- und abbauphase wird aber nur ein sehr geringer Teil ihrer Bandbreite genutzt.

Diesen Nachteil haben eigene Zeichengabernetze nicht. Sie können mit einem einzigen 64 kBit/sec-Kanal etwa 1000 bis 2000 Nutzkanäle gleichzeitig steuern.

Dafür wird ein solcher Nutzkanal zum Zeichengabekanal umfunktioniert. Gemäß einer CCITT-Empfehlung handelt es sich dabei meist um den 16. der insgesamt 32 Kanäle einer 2 MBit-Leitung. Fällt dieser aus, wird ein anderer Nutzkanal belegt.

4.4.3 Routing im ZGS-7

Jeder Zeichengabe-Punkt⁹⁰ wird eindeutig durch einen 14bit langen Zeichengabe-Punkt-Code (signalling-point-code, SPC) gekennzeichnet. Jede Nachricht enthält sowohl den SPC des Ursprungs- (OPC - originating PC) als auch des Ziel-Zeichengabepunkts (DPC - destination PC).

In der Ebene 3 des MTP wird anhand dieser Information jedes eingehende Paket in einem Zeichengabepunkt überprüft, ob es für diesen Punkt bestimmt ist oder nicht. Pakete für andere Zeichengabepunkte werden anhand einer routing-Tabelle⁹¹ weitergeleitet. Dazu verfügt er über eine Tabelle, in der alle möglichen Ziel-Zeichengabepunkte und der zu verwendende Zeichengabeweg eingetragen sind. Jeder Zeichengabepunkt hat mehrere direkte Nachbarn, mit denen er über Zeichengabewege verbunden ist. Zusätzlich sind in der routing-Tabelle deshalb bis zu drei alternative Zeichengabewege eingetragen. Über sie wird bei Ausfall eines Hauptweges umgeleitet.

Die routing-Tabellen sind fest vorgegeben und werden nicht dynamisch an die Last auf einzelnen Streckenabschnitten angepaßt. Das erhöht die Gefahr der lokalen Überlast, obwohl im Netz genügend freie Kapazitäten vorhanden sind. Die Tabellen werden von Wartungspersonal mit Hilfe von Computerprogrammen bestimmt und von Zeit zu Zeit an Veränderungen im Netz angepaßt.

⁹⁰ dazu gehören Zeichengabe-Endpunkte und Zeichengabe-Transferpunkte

⁹¹ vgl. [ban95] Abschnitt 6.3.3.4

4.4.4 Netzübergänge

Die verschiedenen ZGS-7-Netze weltweit sind zunächst gegeneinander abgeschottet. Damit auch Kunden unterschiedlicher Netzbetreiber miteinander telefonieren können, müssen aber Verbindungen zwischen deren Zeichengabernetzen bestehen. Zu diesem Zweck gibt es ganz bestimmte Netzübergänge, sogenannte Gateways. Sie gehören jeweils zwei Zeichengabernetzen an. In beiden Netzen haben sie einen eigenen signalling-point-code (SPC) und eine eigene Zeichengabeverbindung zu den Nachbarn. In den routing-Tabellen in einem Netz wird eingetragen, daß alle Nachrichten, die das Netz verlassen sollen, an einen der Netzübergänge zu schicken sind. Der sendet das Paket seinerseits über seine andere Verbindung in das andere Netz. Das muß nicht unbedingt das Zielnetz sein.

Die festgelegten Netzübergänge geben den Netzbetreibern die Chance, Sicherheitsüberprüfungen einzubauen. Alle Pakete, die einen Netzübergang passieren wollen, werden in mehreren Ebenen überprüft, ob sie den internationalen Normen entsprechen. Erst wenn ein Paket die Prüfungen überstanden hat, wird es in das andere Netz gesendet. Natürlich kann man die Überwachung an dieser Stelle auch auf den Inhalt der Nachrichten ausdehnen.

4.4.5 Das Telekom-Netz

Das Fernsprech- und ISDN-Netz der Telekom umfaßt etwa 6200 Ortsvermittlungsstellen in etwa 4000 Ortsnetzen. Einige Ortsnetze haben also mehrere Vermittlungsstellen. In der Regel werden dann die Teilnehmernummern in Bereiche gleicher Anfangsziffern aufgeteilt.

Die Vermittlungsstellen sind zum Teil direkt mit ihren Nachbarn verbunden. Damit Ferngespräche nicht über eine große Anzahl von Zwischenvermittlungsstellen geleitet werden müssen, gibt es zusätzlich ein eigenes Fernnetz. Es besteht aus etwa 600 weiteren Vermittlungsstellen. An sie sind keine Teilnehmer direkt angeschlossen.

Es gibt auf logischer Ebene zwei dieser Netze: Eins für die Nutzkanäle und ein weiteres für die Steuerkanäle des ZGS-7-Netzes. Physikalisch gesehen benutzt das Zeichengabernetz aber normale Nutzkanäle. Sie werden lediglich für die Zeichengabe reserviert. Das ist zum einen wirtschaftlicher, weil keine eigenen Kanäle vorgehalten werden müssen und zum anderen ausfallsicher, weil jeder beliebige Nutzkanal für die Zeichengabe verwendbar ist.

4.4.6 Das nationale Netz

Zusätzlich zum ZGS-7-Netz der Telekom gibt es in Deutschland noch die unabhängigen Netze der Mobilfunkbetreiber und zunehmend der privaten Festnetzbetreiber. Sie sind ganz ähnlich aufgebaut wie das Telekom-Netz und arbeiten auch mit dem Zeichengabesystem-7. Damit Kunden der verschiedenen Netzbetreiber mit Kunden aus anderen Netzen kommunizieren können, wurde ein deutsches Transfernetz eingerichtet. Es enthält nur Zeichengabe-Transferpunkte und keine Zeichengabe-Endpunkte.

Die folgende Abbildung⁹² zeigt schematisch die deutsche Netzlandschaft. In der Mitte ist das nationale Transfernetz dargestellt. Daran schließen sich die Netze der verschiedenen Netzbetreiber an.

⁹² aus [ban95], Seite 109

In den meisten anderen Ländern gibt es keine nationalen Zwischennetze. Dort werden die Netze der einzelnen Betreiber direkt miteinander und mit dem internationalen Netz verbunden. Das spart zwar die zusätzlichen Kosten, ist aber unsicherer, weil kritische Pakete nicht erkannt und gefiltert werden.⁹³

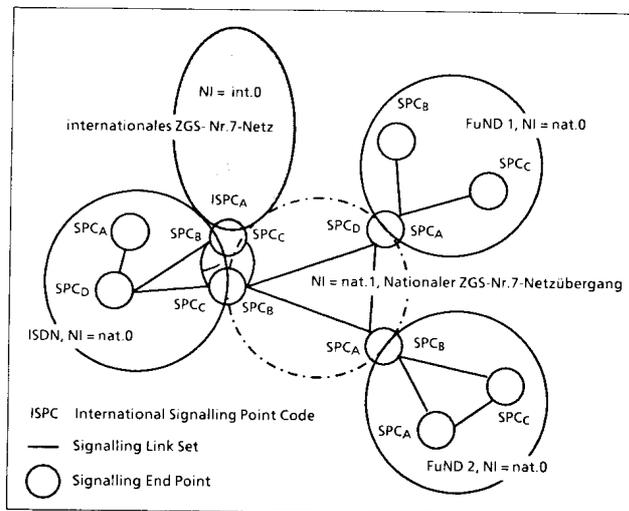


Abb. 6.7 — Struktur des deutschen Zeichengabensystems

4.4.7 Das internationale Netz

Auch auf internationaler Ebene müssen die Betreiber der Telekommunikationsnetze Informationen zur Steuerung ihrer Netze austauschen. Dafür wurde ein eigenes internationales Zeichengabe-Transitnetz geschaffen, das wiederum über Gateways zu allen nationalen Netzen⁹⁴ verfügt. Das internationale Zeichengabe-Transitnetz hat eine eigene Netzkennung: Alle signalling-point-codes dieses Netzes beginnen mit einer 0, alle nationalen mit einer 1. Da nie zwei nationale Netze direkt verbunden sind, dürfen die nationalen SPCs frei vergeben werden, nur die internationalen werden koordiniert.

Nicht alle Telekommunikationsnetze weltweit werden mit dem ZGS-7 betrieben. Deshalb muß das internationale Netz auch über Gateways in Netze mit anderen Zeichengabesystemen verfügen. In den Gateways wird die jeweilige Protokollumsetzung vorgenommen. Die Zusammenarbeit zwischen verschiedenen Netzprotokollen nennt man Interworking.

Das folgende Bild⁹⁵ zeigt schematisch die Funktion des internationalen Transitnetzes und das Zusammenwirken mit den Netzen der einzelnen Länder.

⁹³ siehe Abschnitt 4.6

⁹⁴ bzw. zu den nationalen Transitnetzen, sofern vorhanden

⁹⁵ aus [ban95], Seite 109

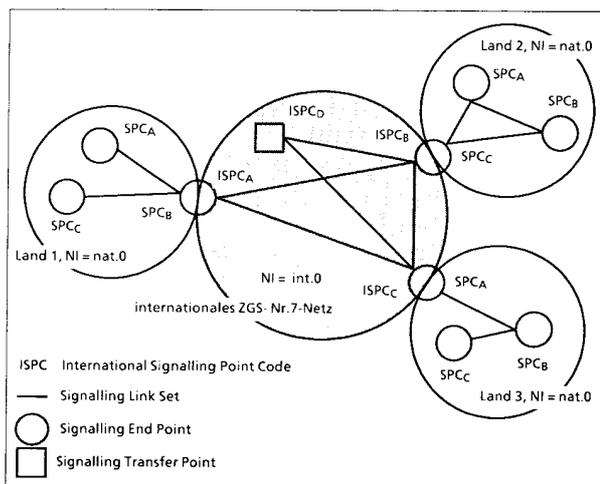


Abb. 6.6 — Struktur des weltweiten Zeichengabernetzes

4.4.8 Interworking⁹⁶

Man kann in einem internationalen Netz wie dem Telefonnetz nicht schlagartig ein neues Zeichengabesystem einführen. Deshalb sind immer mehrere Zeichengabesysteme parallel im Einsatz, manchmal sogar innerhalb eines Landes. Diese Systeme müssen zusammenarbeiten können.

Das Zeichengabesystem 7 setzt sich weltweit immer mehr durch. Daneben gibt es aber noch eine ganze Reihe analoger und ein paar digitale Zeichengabesysteme. Damit Verbindungen zwischen den Netzen mit unterschiedlichen ZGS möglich sind, müssen Schnittstellen geschaffen werden. Das sind Protokollumsetzer in den Vermittlungsstellen, die an zwei verschiedenen Netzen angeschlossen sind.⁹⁷ Ihre Aufgabe ist es, Zeichen gleicher Bedeutung zwischen den Darstellungen in den Systemen zu übersetzen. Das ist aber nicht immer möglich, denn in manchen Zeichengabesystemen gibt es Zeichen, die in anderen nicht vorgesehen sind oder nicht benötigt werden. Unter Umständen muß also ein Zeichen aus dem einen System in mehrere Zeichen des anderen übersetzt werden. Manchmal ist eine Übersetzung auch gar nicht möglich. Dann geht in jedem Fall Information verloren.

Solange nicht in allen Netzen weltweit ein Zeichengabesystem eingesetzt wird, das Sicherheitsfunktionen bietet, kann Sicherheit nicht zum Pflichtteil der Zeichengabe werden: Bei der Umsetzung der Pakete aus einem Netz ohne Sicherheitsunterstützung in ein Netz mit solchen Funktionen müssen Pakete als unsicher gekennzeichnet werden können. Dann kann aber auch ein Angreifer die Sicherheitsmechanismen umgehen.

⁹⁶ vgl. [ban95] Abschnitt 7

⁹⁷ sogenannte gateway-Vermittlungsstellen, siehe Abschnitt 4.4.4

4.5 Ablauf eines Telefonats aus Sicht des Zeichengabesystems

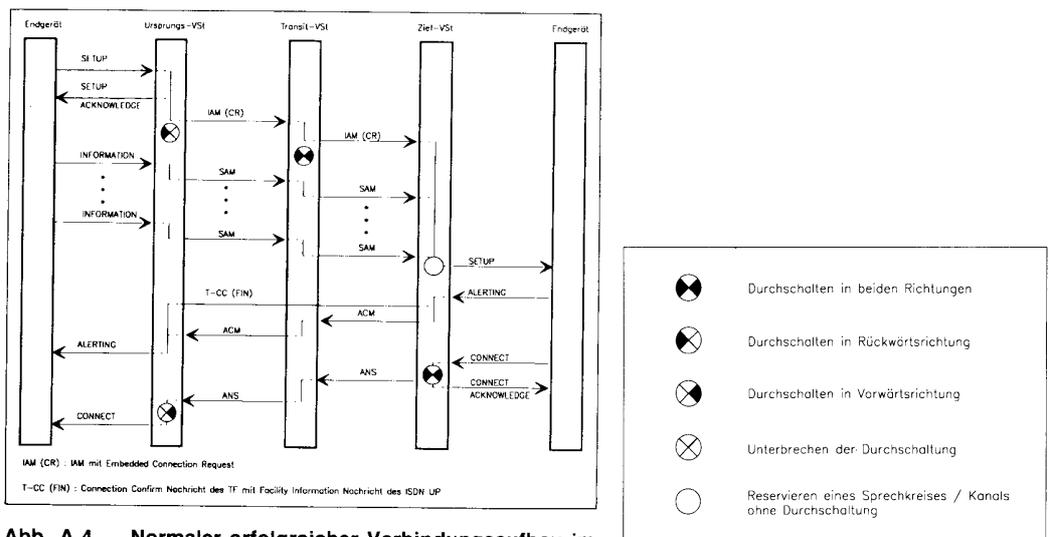


Abb. A.4 — Normaler erfolgreicher Verbindungsaufbau im Netz der Deutschen Telekom (Euro-ISDN)

Abb. A.1 — Übersicht der verwendeten Symbole

aus [ban95] Seite 252

Das linke Bild zeigt exemplarisch den Verbindungsaufbau zwischen zwei Teilnehmern in verschiedenen Ortsnetzen. Der initiierende Teilnehmer A ist links dargestellt, der Angerufene B rechts. Die verwendeten Symbole sind im Bild rechts erklärt.

4.5.1 Zwischen dem Anrufer und seiner Ortsvermittlungsstelle

Der Anrufer A kommuniziert mit seiner Vermittlungsstelle über den D-Kanal seines Anschlusses:

- A nimmt den Hörer ab
- sein Endgerät sendet „setup“ zur Vermittlungsstelle
- diese antwortet mit „setup acknowledge“
- und legt das Freizeichen an den ausgewählten B-Kanal
- In aufeinanderfolgenden „information“-Nachrichten sendet A die Ziffern der Telefonnummer von B
- Wenn es bei B klingelt, sendet die Vermittlungsstelle „alerting“ an A und erzeugt im B-Kanal die hörbaren Klingelzeichen

4.5.2 Zwischen der Ursprungs- und der Transitvermittlungsstelle

Die Vermittlungsstellen untereinander kommunizieren über ZGS-7-Nachrichten:

Die Ursprungsvermittlungsstelle wird im Folgenden mit UVSt, die Transitvermittlungsstelle mit TVSt und die Zielvermittlungsstelle mit ZVSt abgekürzt.

- Sobald die UVSt die „setup“-Nachricht von A erhalten hat, sendet sie eine erste Adressierungs-Nachricht (initial address-message IAM) an die TVSt
- Jede von A eintreffende Wahlziffer wird in einer weiteren Adress-Nachricht (subsequent address message, SAM) an die TVSt durchgereicht
- Diese antwortet, sobald es beim B-Teilnehmer klingelt
- Außerdem schickt die TVSt eine address-complete-message (ACM). Ab dann werden weitere Wahlziffern nicht mehr weitergeleitet oder ausgewertet
- Sobald sich der Angerufene gemeldet hat, sendet die TVSt der UVSt eine „answer“-Nachricht (ANS)

- Jetzt ist der Nutzkanal durchgeschaltet

4.5.3 Zwischen der Transit- und der Zielvermittlungsstelle

Auch hier findet das ZGS-7 Anwendung.

- Die TVSt reicht alle eintreffenden Wahlziffern an die ZVSt weiter
- Die ZVSt reserviert einen Nutzkanal
- Sobald die Rufnummer vollständig ist, wird B gerufen
- Das zeigt die ZVSt der TVSt durch die address-complete-message (ACM) an
- Sobald B den Hörer abhebt, sendet die ZVSt der TVSt eine answer-Nachricht
- Gleichzeitig schaltet sie den Nutzkanal von der TVSt mit dem ausgewählten B-Kanal von B zusammen

4.5.4 Zwischen der Zielvermittlungsstelle und dem Angerufenen

Hier wird wieder über das D-Kanal-Protokoll signalisiert.

- Sobald die Wahlziffern vollständig bei der ZVSt eingetroffen sind, sendet sie eine „setup“-Nachricht an B
- Die kompatiblen Endgeräte bei B antworten mit „alerting“, daß sie klingeln
- Sobald B den Hörer abhebt, sendet das Endgerät „connect“ zur ZVSt
- Die schaltet den Nutzkanal durch und antwortet mit „connect acknowledge“

4.6 Sicherheit im Zeichengabesystem 7

Die Telekommunikationsnetze weltweit bilden zusammen ein hochkomplexes System. Je stärker die Netze verflochten sind, desto größer ist ihre Angreifbarkeit und das mögliche Schadensausmaß. Für die Sicherheit in den Netzen sind die jeweiligen Netzbetreiber selbst verantwortlich. Es darf einem Angreifer nicht gelingen, von irgendeinem Ort in der Welt Telekommunikationsnetze in anderen Ländern zu attackieren.

Das Zeichengabesystem 7 ist aber nicht unter Sicherheitsaspekten entworfen worden. Es verwendet weder Authentisierung noch Verschlüsselung und ist deshalb prinzipiell angreifbar.

Hinzu kommt, daß die ZGS-7-Netze der verschiedenen Ebenen wegen ihrer Komplexität nicht leicht zu überblicken sind. Ein Angreifer kann deshalb darauf hoffen, eine Weile unentdeckt zu bleiben.

Dem versuchen die Netzbetreiber mit folgenden Sicherheitsmaßnahmen zu begegnen:

4.6.1 Transitnetze und Paketfilter in den Netzübergängen

Der wirksamste Schutz ganzer Zeichengabenetze ist das Transitnetz.⁹⁸ Dadurch werden die Netze verschiedener Betreiber voneinander abgeschottet.

An den Grenzen der Netze werden unzulässige Pakete aus dem Datenstrom herausgefiltert. Damit sichern sich die Betreiber gegen verschiedene Angriffe ab: Zum einen gegen die unbefugte und unentgeltliche Benutzung ihrer Netze durch Andere. Zum anderen aber auch gegen Angriffe auf die Stabilität ihres Netzes.

In den USA gibt es solche Netzübergänge nur zum internationalen Netz. Die verschiedenen nationalen Netzbetreiber haben ihre Zeichengabenetze stark vermascht. Ein nationa-

⁹⁸ siehe Abschnitt 4.4.4

les Zeichengabe-Transfernetz wie in Deutschland gibt es dort nicht. Das macht die einzelnen Netze untereinander angreifbar, was in der Vergangenheit auch schon zu großen Problemen geführt hat.

4.6.2 Umleitung bei Ausfall eines Knotens⁹⁹

Ein ZGS-7-Knoten wird so ausgelegt, daß er in 95% aller Fälle etwa zu 20% ausgelastet ist. Bei Ausfall eines Netzknotens kann so der Informationsfluß über einen anderen Knoten umgeleitet werden, ohne diesen gleich zu überlasten.

4.6.3 Lastabwehr

Wenn ein Netz mehr mit Nachrichten zur eigenen Steuerung als mit Nachrichten zur Steuerung von Nutzkanälen beschäftigt ist, wird der Betrieb der Nutzkanäle erheblich gestört. Obwohl dann ausreichend freie Nutzkanäle vorhanden sind, können neue Verbindungen zum Teil nicht aufgebaut werden.

Um zu verhindern, daß das Netz durch Überlast nicht mehr funktionsfähig ist, setzt die Schicht 2 des MTP gezielt Verfahren zur Lastabwehr ein:¹⁰⁰

Wenn ein Zeichengabepunkt überlastet ist, füllt sich sein Eingangspuffer immer mehr. Bei Erreichen einer kritischen Grenze quittiert der Knoten keine empfangenen Nachrichten mehr und sendet statt dessen die Statuskennung für Überlast.¹⁰¹ Dadurch können benachbarte Knoten ihre Pakete aber auch nicht mehr absenden, so daß bei ihnen auch eine Überlast entstehen kann. Lawinenartig könnten so immer mehr Teile des Zeichengabernetzes betroffen werden. Deshalb ist der Zustand „Überlast“ nur für wenige Sekunden erlaubt. Wenn der Zeichengabepunkt danach nicht in den Normalzustand zurückkehrt, wird er vorübergehend außer Betrieb genommen. Die angestauten Informationen in den Nachbarknoten werden dann über alternative Wege geleitet.

4.6.4 Das Überwachungssystem AcceSS7

Das weltweit am häufigsten eingesetzte Sicherheitssystem für das Zeichengabesystem 7 ist AcceSS7 von der Firma Hewlett-Packard.

Es basiert auf Multiprozessor-Rechnern des Typs HP9000 und dem HP-eigenen Unix HP-UX. Die Software ist in C geschrieben. Der Hersteller liefert verschiedene Pakete mit. Sie dienen der Abrechnung, der Abrechnungskontrolle, der Verkehrskontrolle, der Netzplanung, der Auslastungsanalyse und der Betrugsidentifikation. Darüber hinaus kann der Netzbetreiber als Nutzer eigene Software schreiben und so die Funktionen des Systems fast beliebig erweitern.

Von jedem Anruf wird ein Datensatz erzeugt, der sogenannte call-detail-record. Er enthält alle wichtigen Daten über den Anruf, darunter Datum, Uhrzeit, Dauer, anrufender Teilnehmer, angerufener Teilnehmer. Alle Datensätze werden zumindest für eine kurze Zeit gespeichert. Die Auswertungssoftware analysiert die gespeicherten Daten unter beliebigen Kriterien.

Sie kann Benutzerprofile für einzelne Vermittlungsstellen erzeugen und bei Abweichungen sofort Alarm schlagen. Wenn also beispielsweise aus einer einfachen Wohngegend

⁹⁹ Forced Rerouting, erzwungene Umleitung

¹⁰⁰ vlg. [ban95] Abschnitt 6.3.2.9

¹⁰¹ status indication busy (SIB)

urplötzlich eine sehr große Anzahl teurer Auslandsgespräche geführt wird, schlägt die Software Alarm.

Das Alarmsystem basiert dabei auf Mustererkennung:¹⁰² Die Programmierer beschreiben dem System, woran es einen Angriff oder Mißbrauch erkennen kann. Das System durchsucht daraufhin die gespeicherten Daten nach solchen Mustern.

Zum Beispiel können Wählautomaten erkannt werden, weil sie immer exakt gleich lang zwischen zwei Ziffern warten.

Wenn von einem Anschluß in kurzer Zeit eine große Anzahl von gebührenfreien Nummern - womöglich in aufsteigender Reihenfolge - gewählt wird, wird ebenso Alarm geschlagen wie bei besonders vielen kurzen oder einer extrem langen Verbindung.

Ein Operator bekommt die Alarme angezeigt und kann manuell eingreifen.

Daneben stellt AcceSS-7 auch Daten über den Zustand des Nutzkanal- und des Zeichengabernetzes bereit. Alle ZGS-7-Nachrichten werden ebenso wie die Gesprächsdatensätze zwischengespeichert. Sie erlauben so eine nachträgliche Fehleranalyse.

4.7 Angriffe auf das Zeichengabesystem 7

Wie oben erwähnt, werden für das ZGS-7-Netzwerk normale Nutzkanäle verwendet.¹⁰³ Damit könnte das Netz wie folgt angegriffen werden: Ein Angreifer findet eine Fernleitung, klemmt sich auf diese auf und findet diejenige 2Mbit/sec-Leitung heraus, auf deren 16. Zeitschlitz die Zeichengabennachrichten übertragen werden. Das ist zwar unter Umständen sehr zeitaufwendig, weil in Fernleitungen sehr, sehr viele Kupferadern oder zahlreiche Glasfasern geführt sind. Da die Zeichengabekanäle aber besondere Nachrichten übertragen, lassen sie sich anhand ihres Inhalts mit technischer Hilfe von den Nutzkanälen unterscheiden. Die Übertragungsstandards sind frei käuflich und die Zeichengabennachrichten werden unverschlüsselt übertragen.

Wenn ein Angreifer erst einmal den Zeichengabekanal gefunden hat, kann er verschiedene Angriffe probieren:

4.7.1 Künstliche Überlast

Er kann versuchen, das Zeichengabesystem zu überlasten. Dann geht es in die Lastabwehr und einige Teile des Netzes werden automatisch abgeschaltet. So ließen sich beispielsweise ganze Stadtteile vom Telefonnetz abtrennen.¹⁰⁴ Oder Angriffe auf Teilnehmer oder Vermittlungsstellen könnten nicht entdeckt werden, weil die Meldewege blockiert sind.

Dabei gibt es zwei Möglichkeiten, Überlast zu erzeugen: Übermäßig viele Anrufversuche und kreisende Pakete.

Jeder Verbindungsaufbau verursacht eine ganze Reihe von ZGS-7-Nachrichten, auch wenn gar kein Gespräch zustande kommt. Es kann deshalb vorkommen, daß das Telekommunikationsnetz in einem bestimmten Bereich zusammenbricht, wenn zu viele Benutzer gleichzeitig versuchen, Verbindungen aufzubauen. Entweder sind nicht ausreichend Nutzkanäle vorhanden, so daß die Verbindungswünsche abgewiesen werden müs-

¹⁰² pattern matching

¹⁰³ siehe Abschnitt 4.4.1

¹⁰⁴ in diesem Fall funktionieren nur noch katastrophenberechtigte Anschlüsse, siehe Abschnitt 3.9.3

sen oder die Kapazität des Zeichengabernetzes reicht nicht aus. Das ZGS-7-Netz geht dann in die Überlast-Abwehr.¹⁰⁵ Alle neuen Verbindungswünsche werden abgewiesen.

Zeichengabepunkte oder Zeichengabestrecken zwischen zwei Punkten können ausfallen. Damit das Netz dennoch verfügbar bleibt, kennen alle Zeichengabepunkte mehrere alternative Strecken zum Ziel. In den routing-Tabellen wird neben dem Hauptweg immer mindestens eine Alternative eingetragen. Ein Angreifer kann versuchen, die routing-

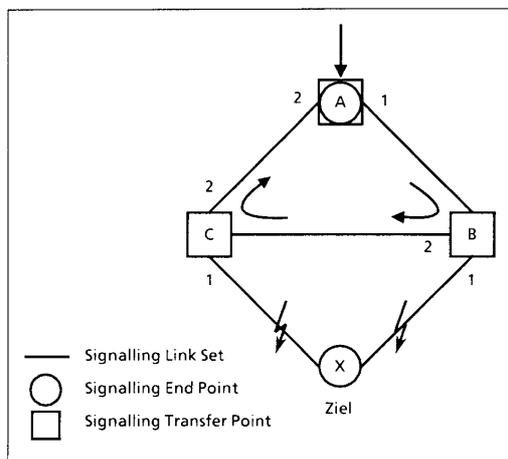


Abb. 6.10 — Kreisrouting wegen Routingfehler im Signalling Point C

Bild: aus [ban95] Seite 112

Tabellen zu manipulieren, so daß kreisende Pakete auftreten.

Da die Pakete in den Knoten sehr schnell bearbeitet und weitergeleitet werden, können schon wenige kreisende Pakete zu Überlast im betroffenen Netzabschnitt führen.

4.7.2 Mißbrauch der Zustandskennungen

In der Schicht 2 des MTP werden auch Statusinformationen zwischen benachbarten Vermittlungsstellen ausgetauscht. Dabei gibt es auch eine Zustandskennung „außer Betrieb“¹⁰⁶ und eine Kennung „Überlast“.¹⁰⁷ Wenn es einem Angreifer gelingt, diese Zustandskennung fälschlicherweise einzuspielen, werden die benachbarten Zeichengabepunkte keine Pakete mehr über den betreffenden Knoten schicken. Er ist dann von der Außenwelt abgeschnitten. Außerdem müssen die anderen Zeichengabepunkte seine Last übernehmen. Das kann bei einem gezielten Angriff schnell zu Überlast führen.

4.7.3 Angriffe aus anderen Zeichengabesystemen

Es reicht nicht aus, die Sicherheit im ZGS-7 zu betrachten. Jedes ZGS-7-Netz hat Übergänge zu Netzen mit anderen Zeichengabesystemen.¹⁰⁸ An den Netzübergängen werden Protokollumsetzungen vorgenommen. Dabei dürfen nur solche Pakete neu erzeugt werden, die im ZGS-7 sicher sind. Unter Umständen kann aber die Sicherheit oder Echtheit einer Nachricht im anderen Zeichengabesystem nicht überprüft werden. Aus Sicherheitsgründen müßte der Protokollumsetzer sie dann verwerfen. Das kann aber die Zusammenarbeit der Netze stark behindern. Hier müssen die Netzbetreiber Kompromisse ein-

¹⁰⁵ siehe Abschnitt 4.6.3.

¹⁰⁶ SIOS, status indication out of service

¹⁰⁷ SIB, status indication busy

¹⁰⁸ siehe Abschnitt 4.4.8

gehen, die Angriffe auf ein ZGS-7-Netz über ein anderes Zeichengabesystem ermöglichen.

4.7.4 Angriffe auf Vermittlungsstellen

Über das Zeichengabernetz lassen sich die Vermittlungsstellen wesentlich leichter angreifen als von der Teilnehmerseite her.

Vermittlungsstellen des Typs S12 von SEL-Alcatel werden über das ZGS-7-Netz ferngesteuert. Dazu wurde das ZGS-7 um einige Protokollelemente erweitert. Prinzipiell kann auch ein Angreifer diese Elemente mißbrauchen.

Die Siemens-Vermittlungsstellen des Typs EWSD werden über ein eigenes Datennetz gesteuert, das physikalisch vom ZGS-7 und vom Telekommunikationsnetz getrennt ist.

4.7.5 Überlisten der Netzübergänge

Jedem service-point-code wird eine Netzkennung vorangestellt. Diese ist zwei Bit lang. Es gibt also weltweit nur vier verschiedene Netzkennungen. Zwei davon sind für das internationale Transitnetz vorgesehen. Sie beginnen mit 0. Die beiden anderen stehen den Netzbetreibern in den Ländern zur Verfügung.

Ein Angreifer kann seine Absenderadresse fälschen, indem er ihr eine falsche Netzkennung voranstellt. Im Netzübergang scheint das Paket dann aus dem Zielnetz zu stammen. Es wird zum Ziel geleitet und dabei nicht überprüft.

Möglich ist ein solcher Angriff, weil die Netzübergänge gleichzeitig auch Transferpunkte innerhalb beider Netze sein können, denen sie angehören.

Nach Aussagen der Telekom wird diese Art von Angriff in den Netzübergängen erkannt und entsprechende Pakete werden herausgefiltert.

5 Bedeutung der Sicherheitslücken und Risiken

In den vorangegangenen drei Kapiteln wurden mögliche Angriffe im ISDN aufgezeigt. Nur ein Teil dieser Angriffe richtet sich gegen die Netzbetreiber, in nur wenigen Fällen tragen sie unmittelbaren Schaden davon. Trotzdem können nur sie viele Sicherheitslücken schließen. Sie setzen selbst Standards und wirken zusammen mit Herstellern und anderen Betreibern in Standardisierungsgremien mit. Wenn dort keine ausreichenden Sicherheitsmaßnahmen festgelegt werden, kann der Kunde nur sehr selten durch eigene Maßnahmen die Sicherheit verbessern.

In Zukunft wird die Sicherheit in den Netzen ein Verkaufsargument der konkurrierenden Netzbetreiber sein.

In diesem Kapitel werden die beschriebenen Angriffe bewertet und gewichtet. Dazu werden zunächst Bewertungskriterien zusammengestellt und anschließend die verschiedenen Angriffstypen anhand der Kriterien eingeordnet.

5.1 Bewertungskriterien

Bei der Bewertung der aufgezeigten Risiken kann man die folgenden Unterscheidungskriterien ansetzen. Die Zuordnung ist dabei nicht immer ganz eindeutig:

5.1.1 Anzahl der Betroffenen

Ein Angriff kann sich gezielt gegen einen Einzelnen richten. Dazu gehören zum Beispiel das Abhören von Räumen oder Gesprächen oder das Erstellen von Kommunikationsprofilen. Es kann aber auch eine Gruppe von Personen gezielt angegriffen werden, zum Beispiel eine geschlossene Benutzergruppe¹⁰⁹ oder eine Firma mit einer oder mehreren ISDN-Anlagen.

Davon muß man Angriffe unterscheiden, die sich gegen ganze Stadtviertel, Vermittlungsstellen, Regionen oder gar gegen ganze Netze richten. Hier sind Personen und Firmen zufällig betroffen. Der eigentliche Angriff richtet sich nicht gegen sie oder nur gegen einen Teil der letztendlich Betroffenen.

Daneben gibt es auch Angriffe, bei denen der Geschädigte nicht gezielt ausgewählt wird. Dazu gehören das Telefonieren auf Kosten Anderer oder der 0190-Betrug.¹¹⁰ Es geht hier nicht darum, jemanden zu schädigen, sondern selbst einen finanziellen Vorteil zu erreichen. Dabei nimmt der Angreifer die Schädigung in Kauf.

5.1.2 Art und Umfang des Schadens

Der Angegriffene kann einen meßbaren finanziellen Schaden haben. Das ist immer dann der Fall, wenn auf seine Kosten telefoniert wird, aber auch wenn Einrichtungen zerstört oder gestohlen werden. Hier kommt unter Umständen auch ein nicht meßbarer Schaden durch entgangene Geschäfte während des Ausfalls hinzu.

Einen nicht immer meßbaren finanziellen Schaden richten Spionageangriffe an. Ein solcher Angreifer hört Räume oder Gespräche ab oder dringt in Rechnersysteme ein. Anschließend verkauft er die gewonnene Information an konkurrierende Unternehmen. Der

¹⁰⁹ GBG, siehe Abschnitt 2.8

¹¹⁰ siehe Abschnitt 3.9.8

Angegriffene hat dadurch Wettbewerbsnachteile, die sich selten genau beziffern lassen, meist aber nicht unerheblich sind.

Außerdem kann es zu einem Vertrauensverlust kommen, wenn durch Spionage vertrauliche Daten in die falschen Hände oder an die Öffentlichkeit geraten. Dazu gehören das Abhören von Räumen oder Gesprächen ebenso wie das Erstellen von Gesprächsprofilen und das Eindringen in Rechnersysteme über das ISDN.

5.1.3 Dauer der Schädigung

Der Schaden, den ein Angriff anrichtet, kann unterschiedlich lange anhalten.

Der Angegriffene wird nur einmal geschädigt, wenn jemand auf seine Kosten telefoniert. Denn sobald die nächste Rechnung eintrifft, fällt der Betrug in der Regel auf.

Dagegen kann beispielsweise das Abhören von Räumen oder Gesprächen beliebig lange stattfinden. Die Chance, daß es entdeckt wird ist meist gering, gerade weil der Täter dazu nicht vor Ort sein muß.

Unter Umständen gibt es Nachwirkungen, die länger andauern, als der Schaden selbst: Firmen im Versandhandel sind auf funktionierende Telefone angewiesen, um Bestellungen entgegennehmen zu können. Wenn dort die TK-Anlage ausfällt, können keine Bestellungen entgegengenommen werden. Einige Kunden werden dann zur Konkurrenz abwandern. Dadurch ist auch dann noch der Betrieb gestört, wenn die TK-Anlage wieder funktioniert.

Für manche Unternehmen bedeutet der Ausfall ihrer Telekommunikationsverbindungen für mehr als ein oder zwei Tage den Konkurs.¹¹¹ Dabei kann der Wiederaufbau einer durch Feuer oder Wasser zerstörten TK-Anlage durchaus Wochen bis Monate in Anspruch nehmen.¹¹²

5.1.4 Verantwortungsbereich

Ein Teil der Angriffe wird nur möglich, weil der Betreiber einer ISDN-TK-Anlage keine ausreichenden Sicherheitsvorkehrungen trifft. Dazu gehören zum Beispiel unveränderte Paßwörter¹¹³ und nicht abgesicherte Fernwartungszugänge.¹¹⁴ Diese Sicherheitslücken liegen im Verantwortungsbereich des Anlagenbetreibers. Er kann sie durch geeignete Maßnahmen abstellen.

Andere Angriffe sind durch Schwachstellen und Sicherheitslücken im Netz möglich. Dazu gehören zum Beispiel die Angriffe auf das ZGS-7-Netz¹¹⁵ und auf die Vermittlungsstellen.¹¹⁶ Die Schwachstellen, die sie ermöglichen, liegen im Verantwortungsbereich des Netzbetreibers. Nur zum Teil kann sich auch der Anlagenbetreiber vor Angriffen auf das Netz schützen.¹¹⁷

Vor einem weiteren Teil der Angriffe kann sich der Nutzer eines ISDN-Endgerätes zumindest zum Teil schützen. Dazu gehören das Abhören von Räumen und das Eindringen in Rechnersysteme mit ISDN-Karten.

¹¹¹ siehe [bsi-94]

¹¹² siehe Abschnitt 2.7.1

¹¹³ siehe Abschnitt 2.7.1

¹¹⁴ siehe Abschnitt 2.7.1.1

¹¹⁵ siehe Abschnitt 4.6

¹¹⁶ siehe Abschnitt 3.9

¹¹⁷ siehe Kapitel 8

5.2 Bedeutung für den Netzbetreiber

5.2.1 Einleitung

In den vorangegangenen Kapiteln wurden Angriffe und Sicherheitslücken auf verschiedenen Ebenen der Telekommunikationswelt betrachtet. Darunter waren immer auch Angriffe, die sich unmittelbar gegen die Netzbetreiber richteten und Angriffe, die sich gegen die Teilnehmer richteten aber im Verantwortungsbereich der Netzbetreiber liegen.

5.2.2 User-user-Mißbrauch

ISDN-Kunden können das Dienstmerkmal User-To-User-Signalling benutzen, um kostenlos Daten über das Netz auszutauschen.¹¹⁸

Diese Daten werden transparent über das ZGS-7-Netzwerk übertragen. Dabei entstehen dem Netzbetreiber Kosten, die er nicht an den Kunden weitergeben kann. Es gibt Überlegungen, schon für den Verbindungsaufbau Gebühren zu nehmen oder User-To-User-Signalling nicht mehr anzubieten.

Wegen der relativ geringen Übertragungsrate von 32 Byte/sec gibt es aber nicht viele ernsthafte Nutzer dieser Lücke. Deshalb hat sich die Telekom bisher darauf beschränkt, den Kunden eine Broschüre zu diesem Thema zuzuschicken. Darin weist sie darauf hin, daß jeder Netzmißbrauch einen Verstoß gegen die allgemeine Geschäftsbedingungen darstellt.

5.2.3 0190-Gebührenbetrug

In Abschnitt 3.9.8 werden mehrere Varianten des Gebührenbetrugs mit 0190-Nummern beschrieben. Ein Teil geht zu Lasten der Kunden, der andere zu Lasten des Netzbetreibers.

Wenn 0190-Gebühren mit Hilfe unbenutzter Anschlüsse verursacht werden, bleibt der Netzbetreiber auf den Kosten sitzen, hat aber in der Regel schon an den Anbieter der Servicenummer gezahlt.

Wenn Telefonanschlüsse von Kunden dafür mißbraucht werden, müssen diese oft die Kosten tragen. In besonders auffälligen und schweren Fällen haben die Gerichte entschieden, daß der Netzbetreiber den Teil der Kosten zu tragen hat, der über die normale Telefonrechnung hinausgeht.

Auch wenn der Kunde betroffen ist, kann hauptsächlich der Netzbetreiber etwas gegen diese Angriffsmöglichkeit tun. Der Kunde kann nur dafür sorgen, daß sich niemand innerhalb seines Machtbereichs, also an seiner Hausinstallation aufklemmt. Dem Netzbetreiber obliegt dagegen der Schutz der Leitung zwischen Kunde und Vermittlungsstelle. Sie ist oft einige Kilometer lang und durchläuft mehrere Verteilerkästen. Das Aufklemmen fällt hier nicht sonderlich schwer, auch wenn die Verteilerkästen nur mit Spezialwerkzeug geöffnet werden können.

Soweit bekannt, wurden alle 0190-Betrugsfälle mit Hilfe analoger Telefonanschlüsse und automatischen Wählern durchgeführt worden. Im Rahmen des ISDN ist der Aufwand für einen solchen Angriff größer als der zu erwartende Nutzen.

¹¹⁸ siehe Abschnitt 3.9.7

Der Grund dafür liegt darin, daß zwischen der Vermittlungsstelle und dem Teilnehmeranschluß ein anderes Protokoll verwendet wird, als zwischen dem Teilnehmeranschluß (NT) und den Endgeräten. Im einen Fall kommt das D-Kanal-Protokoll zum Einsatz, im anderen Fall der S₀-Bus. Deshalb kann man keine normalen Endgeräte außerhalb des Hauses oder der Wohnung des Teilnehmers an die Leitung anschließen.

Auch wenn bisher im ISDN keine solchen Betrugsfälle bekannt geworden sind, sind sie dennoch möglich: Mit Hilfe eines manipulierten Prüftelefons kann sich ein Angreifer in die Leitung hängen und beliebige Anschlüsse anwählen. Dann ist aber der Teilnehmer für diese Zeit vom Netz abgeklemmt. Ein solcher Angriff kommt also nur nachts oder während des Urlaubs des Teilnehmers in Frage.

Die Kosten für ein Prüftelefon betragen etwa 1000,- DM; dem gegenüber kostet ein automatisches Wählgerät nur etwa 100,-DM. Deshalb werden sich solche Angriffe auf nicht-ISDN-Anschlüsse konzentrieren. Das ist nach wie vor die weit überwiegende Zahl.

5.2.4 Netzausfall durch Sabotage

Es gibt eine Reihe von Angriffen, die sich gegen die Qualität des Netzes richten. Im schlimmsten Fall wird einem oder mehreren Nutzern der Dienst ganz verweigert. Diese Angriffe werden unter dem Begriff denial-of-service zusammengefaßt.

Wenn es einem Angreifer gelingt, eine Vermittlungsstelle unter seine Kontrolle zu bringen, kann er sie in einen unsinnigen Zustand versetzen, so daß alle angeschlossenen Benutzer keine Verbindungen mehr bekommen können.

Dabei sind aber einige Hürden zu nehmen. Ein Zugriff über das ZGS-7-Netz kann mit dem Access-7-System erfaßt werden. Über den D-Kanal kann nur angegriffen werden, wenn vorher eine Sicherheitslücke entdeckt oder gezielt eingebaut wurde. Und ein physikalisches Eindringen in die Vermittlungsstelle wird über ein Alarm- und Protokollsystem gemeldet. Außerdem benötigt der Angreifer dann noch ein gültiges Paßwort zum Zugriff auf den Konfigurationsrechner. Deshalb stellen in diesem Fall Innentäter die größte Gefahr dar.

Eine andere Art des Angriffs stellen physikalische Beschädigungen dar. Auch sie haben zum Ziel, den Netzbetrieb zu stören:

1995 wurden am Frankfurter Flughafen einige Glasfaserleitungen durchtrennt. Die Reparatur dauerte einen ganzen Tag. Einige Anwohner flughafennaher Stadtteile hatten solange keine Telefonverbindung. Für den Flughafen selbst wurden weitestgehend Ersatzschaltungen durchgeführt. Eine Ersatzschaltung ist immer dann möglich, wenn es zwischen zwei Knotenpunkten im Netz mehr als eine Verbindung gibt. Beim Ausfall einer Verbindung wird der gesamte Verkehr über die andere umgeleitet. Dabei kann es zu kurzzeitiger Überlast kommen. Über solche Ersatzschaltungen verfügen jedoch nur wichtige Einrichtungen und die Fernverbindungen, deren Ausfall sonst ganze Regionen lahmlegen könnte.

Die Fernleitungen sind mit einer zusätzlichen Ummantelung versehen. Zwischen dieser und der eigentlichen Kabelummantelung wird Druckluft geführt. Wird ein Kabel beschädigt, so fällt schlagartig der Druck ab. Durch Meßgeräte kann man die beschädigte Stelle sehr schnell und präzise eingrenzen. Ohne diese Technik würde es Wochen dauern und viel Geld kosten, eine Beschädigung aufzuspüren.

Bei einem Angriff können auch Vermittlungsstellen oder Straßenverteiler beschädigt werden. Der Ausfall eines Straßenverteilers schneidet den angeschlossenen Straßenzug

völlig vom Netz ab. Ersatzschaltungen sind nicht möglich, weil ab dem Straßenverteiler genau eine physikalische Leitung je Anschluß vorhanden ist. Die Installation eines neuen Verteilers kann in wenigen Tagen erfolgen, wenn die Kabel intakt geblieben sind. Wenn neue Kabel in die Häuser verlegt werden müssen, vergehen Wochen bis der Urzustand wiederhergestellt ist.

Der Ausfall einer Vermittlungsstelle schneidet alle daran angeschlossenen Teilnehmer vom Rest des Telekommunikationsnetzes ab. Wenn nur die Verbindungen von der Vermittlungsstelle ins Fernnetz ausfallen, können die betroffenen Teilnehmer nur noch mit anderen Teilnehmern an der selben Vermittlungsstelle kommunizieren. Gespräche von und nach außerhalb sind nicht mehr möglich. Wenn die Vermittlungsstelle völlig ausfällt, können die angeschlossenen Teilnehmer gar nicht mehr kommunizieren. Das können bis zu zehntausend Anschlüsse sein.

Bis eine Vermittlungsstelle wiederhergestellt ist, vergehen im besten Fall Stunden, im schlimmsten Fall Monate. Das Einspielen und Aktivieren einer neuen Software dauert nur ein paar Stunden. Wenn auch die Konfiguration aller Teilnehmeranschlüsse wiederhergestellt werden muß, können Tage vergehen. Wenn die Vermittlungsstelle durch Feuer oder Wasser beschädigt wurde, dauert es Monate, bis zur vollständigen Wiederherstellung. Denn dann muß neue Hardware installiert und alle Teilnehmerleitungen neu aufgeschaltet („rangiert“) werden.

Eine Ersatzschaltung ist nicht möglich, weil die Teilnehmeranschlußleitungen physikalisch von der Vermittlungsstelle aus über Straßenverteiler zum Kunden verlaufen. Im Prinzip ist ab der Vermittlungsstelle jedem Kunden eine eigene Kupferdoppelleitung fest zugeordnet.

Lediglich zwischen Vermittlungsstelle und einem Straßenverteiler kann ersatzgeschaltet werden, wenn nur eine oder wenige Teilnehmerleitungen - beispielsweise bei Bauarbeiten - beschädigt werden.

5.2.5 Aufklemmen auf D-Kanal oder das ZGS-7

Eine ganz andere Gefahr droht den Vermittlungsstellen durch Angriffe über eine ihrer Leitungen. Das können sowohl die Leitungen aus Richtung der Teilnehmer als auch die Leitungen aus Richtung des Fernnetzes sein.

Aus Richtung der Teilnehmer droht Gefahr über den D-Kanal. Die B-Kanäle werden als reine Nutzkanäle zwischen den Kommunikationspartnern transparent durchgeschaltet und in den Vermittlungsstellen nicht ausgewertet.

Ein Angreifer kann ungültige Pakete über den D-Kanal eines Anschlusses zur Vermittlungsstelle schicken. Das können zu kurze, zu lange oder einfach nicht spezifizierte Pakete sein. Die Chancen, damit Schaden in der Vermittlungsstelle anzurichten, sind allerdings gering. Denn gegen unspezifizierte Pakete wird die Vermittlungsstellen-Software vor der Freigabe geprüft. Dazu enthalten alle ETSI-Spezifikationen einen eigenen Abschnitt, der beschreibt, welche Arten von Paketen zu prüfen und zu verwerfen sind. Ein Angreifer kann allerdings in den ETSI-Dokumenten nach Lücken suchen und hoffen, daß diese Pakete nicht geprüft werden.

Größere Chancen auf Erfolg bestehen bei vorher manipulierter Vermittlungsstellen-Software.¹¹⁹

¹¹⁹ siehe Abschnitt 5.2.8

Aus Richtung des Fernnetzes drohen den Vermittlungsstellen mehr Gefahren. Denn dem Fernnetz wird grundsätzlich erst einmal vertraut, während Paketen von Seiten der Teilnehmer grundsätzlich erst einmal mißbraut wird.

Wenn es einem Angreifer also gelingt, in das ZGS-7-Netz manipulierte Pakete einzuspielen, so steht ihm jede Vermittlungsstelle offen. Er kann dann die Vermittlungsstelle veranlassen, irgendwelche Pakete über den D-Kanal in Richtung eines bestimmten Teilnehmers zu schicken. Damit ist wiederum ein gezielter Angriff auf den Teilnehmer möglich. Denn die Teilnehmer-Hardware vertraut den aus der Vermittlungsstelle empfangenen Paketen grundsätzlich.

Bei Vermittlungsstellen von SEL können so auch Teilnehmeranschlüsse in der Vermittlungsstelle umkonfiguriert werden, denn SEL verwendet ein leicht verändertes ZGS-7-Protokoll für die Fernwartung seiner Vermittlungsstellen.¹²⁰

Von einem solchen Angriff sind entweder einzelne oder alle Teilnehmer an der angegriffenen Vermittlungsstelle betroffen. Bis eine Manipulation entdeckt wird, kann schon einige Zeit vergehen. Ein Angreifer kann darauf hoffen, daß ihm die Größe des Netzes zu Hilfe kommt: Ein weltweites Telekommunikationssystem, bestehend aus vielen Netzen und anderen Gliederungsformen, ist nicht leicht zu überblicken.

Wenn eine Vermittlungsstelle erst einmal unter der Kontrolle eines Angreifers ist, kann er sie veranlassen, andere Vermittlungsstellen anzugreifen. Die Vermittlungsstellen eines Netzes vertrauen einander, eingehende Pakete werden nicht geprüft. Auf diese Weise läßt sich virenartig das gesamte ZGS-7-Netz unter Kontrolle bringen. Die Gefahr, entdeckt zu werden, wächst allerdings mit der Anzahl der angegriffenen Vermittlungsstellen. Im Prinzip kann ein Angreifer aber auf diese Weise von einem beliebigen Ort aus einen Teilnehmer an einem beliebigen anderen Ort angreifen.

5.2.6 Überlast im ZGS-7-Netz

Ein Angreifer kann das ZGS-7-Netz durch Angriffe überlasten.¹²¹ Das Netz wird daraufhin keine neuen Verbindungswünsche mehr annehmen. Auf diese Weise lassen sich ganze Stadtteile oder Regionen lahmlegen.

Zum Angriff auf das ZGS-7-Netz ist neben einer Menge Spezialwissen und spezieller Hardware der Zugriff auf das Netz nötig. Dann kann ein Angreifer relativ leicht Pakete aussenden und zum Beispiel Überlast erzeugen. Ein solcher Angriff dürfte einem Innentäter nicht schwer fallen. Allerdings ist die Chance (oder das Risiko) relativ hoch, daß er vom AcceSS7-System¹²² erfaßt wird.

Außerdem können auf dieser Ebene Ersatzschaltungen aktiviert werden, so daß ein solcher Angriff nur kurzzeitig zu Ausfällen führt. Es sei denn, auch die Ersatzwege sind betroffen. Ein groß angelegter Angriff kann durchaus das gesamte Netz lahmlegen. Bis sich die Situation durch manuellen Eingriff normalisiert hat, können Stunden vergehen.

5.2.7 SEPT-Mißbrauch

In Abschnitt 3.9.1 wird die System-externe-Prüf-Technik (SEPT) beschrieben. Ein Angreifer benötigt lediglich eine vierstellige Technikererkennung und ein ebenfalls vierstelli-

¹²⁰ Siemens verwendet ein eigenes, physikalisch getrenntes Netz.

¹²¹ siehe Abschnitt 4.7.1

¹²² siehe Abschnitt 4.6.4

ges Paßwort. Beide lassen sich durch Versuche herausbekommen oder von einem In-entäter kaufen.

Bislang fehlen technische Mittel, um den Zugriff auf SEPT sicherer zu gestalten. Denn jeder Techniker soll von überall mit Hilfe eines normalen Telefonanschlusses Prüfroutinen anstoßen können. Er hat keine andere Möglichkeit, sich gegenüber dem System zu legitimieren, als durch Eingabe eines Paßworts, das systembedingt nur aus Ziffern bestehen kann.

Einen gewissen Schutz bieten die abgestuften Berechtigungen der Benutzerkennungen im SEPT: nicht jeder darf alles. Insbesondere das Aufschalten auf eine bestehende Verbindung bleibt besonders privilegierten Technikern vorbehalten. Ein weiterer Schutzmechanismus ist die lokal begrenzte Gültigkeit der Zugangskennungen: Sie gelten immer im Umkreis von 40-70 Kilometern um eine Vermittlungsstelle. Wer sich also beispielsweise von München aus auf einen Hamburger Anschluß aufschalten will, benötigt eine für Hamburg gültige Kennung.

Wenn ein Angreifer aber erst einmal eine privilegierte Kennung mitsamt Paßwort hat, kann er gezielt jeden Anschluß innerhalb des Gültigkeitsbereichs angreifen und Gespräche aus der Ferne abhören.

5.2.8 Vermittlungsstellensoftware

Ein besonderes Problem stellt die Vermittlungsstellensoftware dar. Wie in Abschnitt 3.8.1 beschrieben, ist sie schon Jahrzehnte alt und für einen Einzelnen nicht zu durchschauen. Mit Hilfe eines Mittäters beim Softwarehersteller kann ein Angreifer dafür sorgen, daß in der nächsten Softwareversion ein Hintertürchen eingebaut wird. Er hat gute Chancen, unentdeckt zu bleiben. Denn beim Softwarehersteller und beim Abnehmer¹²³ wird die Software nur getestet, nicht aber verifiziert. Dabei wird geprüft, ob das Verhalten den ETSI-Normen entspricht, auch wenn unzulässige Nachrichten auszuwerten sind. Eine echte Verifikation ist bei dem Umfang und der Struktur der Software auch gar nicht möglich.

Wenn das Hintertürchen erst einmal eingebaut ist, muß der Angreifer nur abwarten, bis die Software in den Vermittlungsstellen installiert wurde. Das dauert maximal ein Jahr. Danach stehen dem Angreifer alle Anschlüsse im gesamten Netz zur Verfügung, die an dem manipulierten Vermittlungsstellen-Typ angeschlossen sind. In Deutschland gibt es nur zwei Hersteller von Vermittlungsstellen: Siemens und SEL Alcatel. An welchem Vermittlungsstellen-Typ ein bestimmter (anzugreifender) Anschluß hängt, kann man in T-Online oder durch einen (kostenlosen) Anruf beim Kundenservice¹²⁴ herausfinden. Der Netzbetreiber gibt dort bereitwillig Auskunft.

Wer erst einmal die Vermittlungsstellen unter seine Kontrolle gebracht hat, kann nach Belieben Anschlüsse umkonfigurieren, auf Kosten Anderer telefonieren, Verbindungen überwachen und Gespräche und Datenübertragungen abhören.

5.3 Bedeutung für den Kunden

Die meisten der geschilderten Angriffe haben auch Auswirkungen auf Kunden. Die Betroffenen können abgehört oder ausspioniert werden, aus ihrem Gesprächsverhalten können Profile erstellt werden, Andere können auf ihre Rechnung telefonieren oder ihre

¹²³ Das ist der Netzbetreiber

¹²⁴ Telefon 01114

ISDN-Anlage lahmlegen. Wenn Computernetze und Telefonanlagen miteinander verbunden sind, ist über das eine Netz ein Angriff auf das andere möglich.

5.3.1 Abhören von Gesprächen

Ein Angreifer hat verschiedene Möglichkeiten, die Kommunikation eines ISDN-Teilnehmers abzuhören:

Ein Gespräch im ISDN läuft über mehrere Stationen: Vom Endgerät vieradrig über den S_0 -Bus zum Netzabschluß (NT), von dort zweiadrig über die Teilnehmer-Anschlußleitung zur Vermittlungsstelle. Dort wird es über einen der zahlreichen Nutzkanäle zur nächsten Vermittlungsstelle weitergeleitet. So nähert es sich der Zielvermittlungsstelle. Dort folgt der Weg über die Teilnehmer-Anschlußleitung und den S_0 -Bus beim Zielteilnehmer.

Ein Angreifer hat verschiedene Möglichkeiten, die unterschiedlich aufwendig, erfolgversprechend und weitreichend sind: Er kann den S_0 -Bus, die Teilnehmeranschlußleitung, Teilnehmerports in den Vermittlungsstellen oder Fernleitungen abhören.

Sowohl beim Anrufer als auch beim Angerufenen laufen Gespräche, Faxe und Daten über den S_0 -Bus. Jeder Bus ist leicht abzuhören, wenn man direkten physikalischen Zugriff auf ihn hat. Man kann einfach ein manipuliertes zusätzliches Endgerät an den Bus anschließen und damit sowohl den D-Kanal als auch die B-Kanäle am Bus abhören. Von einem solchen Angriff ist immer ein einzelner Teilnehmeranschluß betroffen. Die eigentliche Hürde ist der notwendige Zugriff auf den Bus in den Räumen des Teilnehmers. Deshalb ist die Entdeckungsgefahr hier auch recht hoch.

Technisch aufwendiger aber auch mit geringerem Entdeckungsrisiko ist das Abhören der Teilnehmer-Anschlußleitung zwischen der Vermittlungsstelle und dem Teilnehmeranschluß. Sie erreicht schnell eine Länge von mehreren Kilometern. An irgendeiner Stelle kann sich der Angreifer mit Hilfe spezieller Hardware auf die Leitung klemmen und gezielt einen der B-Kanäle abhören. Auch hier ist ein einzelner Teilnehmeranschluß betroffen. Der Zugriff auf die Leitung ist relativ leicht. In den Verteilerkästen sind alle Leitungen übersichtlich aufgereiht und beschriftet. Das Entdeckungsrisiko ist gering, so daß ein solcher Angriff über einen längeren Zeitraum möglich ist.

Gezielten Zugriff auf alle Teilnehmer einer Vermittlungsstelle hat ein Angreifer, wenn er sich in der Vermittlungsstelle befindet. Hier kommen die Zweidrahtleitungen der Teilnehmer an. Sie werden bei einem Gesprächswunsch mit einer der Fernleitungen verbunden. Allerdings werden die Vermittlungsstellen überwacht. Ein Einbruch ist also immer mit einem hohen Entdeckungsrisiko verbunden. Einem Innentäter sollte es aber gelingen, Manipulationen vorzunehmen. Die Schaltschränke in einer Vermittlungsstelle sind sehr unübersichtlich, so daß eine installierte Zusatzhardware mit hoher Wahrscheinlichkeit eine Weile nicht entdeckt wird.

Ein noch größerer Teilnehmerkreis ist abhörbar, wenn sich ein Angreifer auf die Fernleitungen aufschaltet. Sie führen über viele Kilometer quer durch das Land. Ein Angriff kann an einer beliebigen Stelle erfolgen. Hier muß mit Hilfe spezieller Hardware gezielt einer der dreißig Nutzkanäle einer Zweidrahtleitung herausgefiltert werden. Dann kann man das darüber geführte Gespräch abhören. Erheblich leichter lassen sich die Richtfunkstrecken abhören: Ein großer Teil der Telekommunikation wird über weite Strecken per Richtfunk geführt. Irgendwo zwischen Sender und Empfänger kann man eine geeignete Antenne aufstellen und mit Hilfe geeigneter Hardware alle dort übertragenen Gespräche abhören.

Um herauszufinden, wer auf der belauschten Leitung gerade mit wem kommuniziert, muß der Angreifer außerdem den dazugehörigen ZGS-7-Kanal finden und analysieren.

Auf diese Weise können aber keine Ortsgespräche abgehört werden, denn sie benutzen die Fernleitungen nicht. Hinzu kommt der besondere Schutz der Fernleitungen durch eine Druckluftüberwachung.¹²⁵

5.3.2 Abhören gespeicherter Nachrichten

Viele Unternehmen benutzen Voice-Mail-Systeme. Die Zugänge zu den Nachrichtenspeichern der einzelnen Teilnehmer sind oft nur mit Standardpaßwörtern abgesichert. In den Speichern können sich sowohl Sprachnachrichten wie in einem herkömmlichen Anrufbeantworter als auch Faxe oder Dateien befinden. Ein Angreifer kann diese Nachrichten abhören, kopieren und weiterverwerten, ohne daß der Angegriffene davon etwas merkt. Für ihn liegen die Nachrichten weiterhin bereit.

Wenn der Angreifer sogar über den Administrationszugang zu einer Anlage verfügt, braucht er nicht die einzelnen Paßwörter der Benutzer. Ihm liegen dann alle Nachrichten des gesamten Unternehmens offen. Betroffen sind damit bis zu mehreren tausend Benutzern, je nach Firmengröße. Die Betroffenen merken den Angriff nicht. Er kann sich also über einen längeren Zeitraum erstrecken. Der mögliche Schaden ist dabei nicht unmittelbar meßbar, kann aber sehr groß werden, wenn sich unter den abgehörten Daten Firmengeheimnisse befinden, die in die Hände der Konkurrenz geraten. Für die Sicherheit des Voice-Mail-Systems sind der Betreiber - also das Unternehmen - und die Nutzer - also die Mitarbeiter - verantwortlich.

5.3.3 Abhören von Räumen

Mit Hilfe von ISDN-Telefonen mit Freisprecheinrichtung lassen sich auch Räume abhören, wie in Abschnitt 2.6.2 beschrieben. Einem Angreifer muß es gelingen, das Freisprechemikrofon im angegriffenen Telefon zu aktivieren. Dazu hat er verschiedene Möglichkeiten:

Unter Umständen bietet eine ISDN-Anlage bereits alles, was er braucht: Das Leistungsmerkmal Direktansprechen. Voraussetzungen sind, daß sich der Angreifer innerhalb der selben ISDN-Anlage befindet wie der Angegriffene, die Berechtigung zum Direktansprechen besitzt und es ihm gelingt, den Aufmerksamkeitston zu unterbinden. Dazu benötigt er Zugriff auf die Anlagenprogrammierung.

Wenn er keinen Zugriff auf die Anlage hat, aber in den abzuhörenden Raum gelangen kann, steht ihm folgende Variante offen: Solange niemand im Raum (beispielsweise Konferenzraum) ist, ruft der Angreifer von dort aus einen beliebigen Anschluß innerhalb oder außerhalb der Anlage an und aktiviert Freisprechen. Der Angerufene kann dann den Raum abhören.

In beiden Fällen muß der Angreifer aber wenigstens Zutritt zum Gebäude des Angegriffenen haben. Deshalb ist das Entdeckungsrisiko recht hoch und der Angriff nicht beliebig oft wiederholbar.

Wenn es einem Angreifer gelingt, das Mikrofon eines Telefons von Außen über geeignete D-Kanal-Befehle zu aktivieren, sind seine Erfolgchancen ungleich höher. Dazu muß er eventuell einmal Zutritt zur Anlage haben, um sie zu manipulieren.

¹²⁵ siehe Abschnitt 5.2.4

5.3.4 Angriffe über den D-Kanal

Wenn ein Angreifer erst einmal eine Vermittlungsstelle unter seiner Kontrolle hat,¹²⁶ kann er sie veranlassen, auch Teilnehmer anzugreifen: Er läßt geeignete D-Kanal-Nachrichten zu den Teilnehmern schicken, um sie so abzuhören oder ihre ISDN-Anlage zu manipulieren. Die Teilnehmer-Endgeräte trauen den Paketen aus der Vermittlungsstelle blind, so daß ein solcher Angriff gute Erfolgchancen hat. Der Teilnehmer wird davon nichts merken.

Auch ohne die Manipulation einer Vermittlungsstelle kann angegriffen werden: Der Angreifer kann sich mit Hilfe spezieller Hardware zwischen Vermittlungsstelle und Teilnehmer auf die Anschlußleitung klemmen und ebenfalls feindliche Pakete zum Teilnehmer schicken. Hierfür benötigt er allerdings eine aufwendigere Hardware als für das Abhören des Teilnehmers auf der Anschlußleitung.

5.3.5 Angriffe auf Rechner/Rechnernetze

Nahezu alle Unternehmen verfügen heute über vernetzte Rechner und über eine ISDN-TK-Anlage. Wenn es Schnittstellen zwischen beiden Systemen gibt, kann ein Angreifer über das eine System kommen und das andere angreifen. Aus Sicherheitsgründen ist das Rechnernetz oft nur lokal erreichbar oder über eine Firewall nach außen abgesichert. Das nützt aber nur wenig, wenn ein Angreifer aus der ganzen Welt in die ISDN-Anlage eindringen kann, und diese eine Verbindung zum Rechnernetz hat. In vielen Arbeitsplatz-PCs sind neben einer Netzwerkkarte auch ein Modem oder eine ISDN-Karte installiert. Sie alle stellen einen potentiellen Übergang zwischen den Systemen und damit eine Schwachstelle dar. In einigen Unternehmen ist es deshalb verboten, eine Modem- und eine Netzwerkverbindung gleichzeitig zu besitzen. Bevor der Anwender sein Modem an die Telefondose anschließt, muß er seine Netzwerkleitung kappen. Ob das in der Praxis geschieht, darf bezweifelt werden.

Außerdem kann ein Angreifer über die Modemverbindung Viren in einen Rechner einschleusen, die ihm die gewünschten Daten aus dem Netz zusammentragen und beim nächsten Anruf automatisch übertragen.

5.3.6 Telefonieren auf fremde Rechnung

Bisher wurden verschiedene Möglichkeiten beschrieben, auf fremde Rechnung zu telefonieren:

Wählautomaten sind kleine Geräte, die auf eine analoge Leitung geklemmt werden und dann selbständig „telefonieren“. Sie werden hauptsächlich für den 0190-Gebührenbetrug benutzt.¹²⁷

Ein Angreifer im ISDN kann sich auf den S_0 -Bus eines Teilnehmers aufklemmen. Von dort aus kann er leicht auf dessen Kosten telefonieren. Aber dazu muß er Zugang zu den Räumen des Teilnehmers haben, denn der S_0 -Bus wird nur zwischen den Endgeräten und dem Netzabschluß beim Teilnehmer verwendet. Dann kann der Angreifer aber genauso gut die Telefone des Teilnehmers benutzen.

Statt dessen kann sich ein Angreifer auch auf die Teilnehmer-Anschlußleitung zwischen dem Teilnehmer und der Vermittlungsstelle aufklemmen und auf dessen Kosten telefonie-

¹²⁶ siehe Abschnitt 5.2.5

¹²⁷ siehe Abschnitt 5.2.3

ren. Dazu benötigt er Zugriff auf die Leitung und spezielle Hardware. Der Zugriff auf die Leitung ist nicht schwierig, die benötigte Hardware kostet etwa tausend Mark. Damit ist sie bedeutend teurer als für einen vergleichbaren Angriff im analogen Netz. Deshalb wird diese Form des Angriffs keine große Rolle spielen, solange die Zahl der ISDN-Anschlüsse geringer ist als die der analogen Anschlüsse.

Auch und gerade im ISDN interessant ist dagegen das Telefonieren über Voice-Mail-Systeme.¹²⁸ Firmen stellen ihren Außendienstmitarbeitern einen kostenlosen Zugang zum Firmentelefonnetz zur Verfügung. Nach Eingabe ihrer persönlichen Kennung und Geheimzahl können die Anrufer oft auch auf Firmenkosten nach Außen telefonieren. Mit zunehmender Verbreitung großer ISDN-Anlagen mit vielen Komfortmerkmalen wächst auch die Zahl dieser Systeme. Damit werden solche Anlagen auch immer attraktiver für Angreifer.

Die Nummern probieren sie aus, spionieren sie an öffentlichen Telefonen oder entnehmen sie weggeworfenen Listen aus den Mülleimern der Unternehmen.

Betroffen sind alle Unternehmen, die über eine solche Anlage verfügen. Sie werden in der Regel nicht gezielt ausgewählt, um sie zu schädigen. Vielmehr suchen die Angreifer nach einer Möglichkeit, auf Kosten irgendeiner Firma zu telefonieren. Wenn sie erst einmal einen Zugang gefunden haben, können sie meist ein paar Wochen unbehelligt telefonieren, bis der Betrug auffällt. Nur wenige Unternehmen haben ein Alarmsystem in ihrer Anlage installiert.¹²⁹

5.4 Datenschutzrechtliche Aspekte

5.4.1 In den Vermittlungsstellen

Verschiedene ISDN-Leistungsmerkmale bieten Mißbrauchsmöglichkeiten, die datenschutzrechtlich bedenklich sind. Dazu gehören CLIP fest¹³⁰ und die overwrite-Berechtigung von Notrufabfrageplätzen.¹³¹

Ein Angreifer kann durch Manipulation in der Vermittlungsstelle bei einem Teilnehmer die Rufnummern-Übermittlung dauerhaft einschalten. Bei jedem Gespräch, das der Angegriffene führt, sieht der Angerufene dessen Rufnummer. Der Angegriffene weiß davon nichts. Dieser Angriff ist nicht nur im ISDN sondern auch bei allen analogen Anschlüssen an digitalen Vermittlungsstellen möglich. Betroffen ist immer ein einzelner Anschluß. Dem Inhaber entsteht kein unmittelbar meßbarer Schaden.

Interessanter ist für einen Angreifer der umgekehrte Fall: Ebenfalls durch Manipulation in der Vermittlungsstelle kann er für seinen eigenen Anschluß die Overwriteberechtigung aktivieren. Dafür benötigt er Zutritt zur Vermittlungsstelle oder einen verbündeten Innentäter. Zutritt zur Vermittlungsstelle ist für Außenstehende praktisch nicht zu bekommen. Aber ein bestechlicher Mitarbeiter des Netzbetreibers könnte die Manipulation vornehmen. Dann sieht der Teilnehmer immer die Rufnummer aller Anrufer, auch wenn diese die Übermittlung unterdrücken. Die Anrufer merken davon nichts. Sie tragen auch keinen unmittelbar meßbaren Schaden davon. Diese Manipulation hat gute Chancen, nie entdeckt zu werden.

¹²⁸ siehe Abschnitt 3.9.5.2

¹²⁹ vgl. [hau96]

¹³⁰ siehe Abschnitt 3.9.3

¹³¹ siehe Abschnitt 3.9.3

5.4.2 In ISDN-Anlagen

Innerhalb von ISDN-TK-Anlagen stehen weitere Merkmale zur Verfügung, die sich datenschutzrechtlich mißbrauchen lassen. Dazu gehören Rückruf im Freifall und Rückruf im Besetztfall. Beide ermöglichen eine Kontrolle der Mitarbeiter.

Der Rückruf im Freifall erlaubt es - in Grenzen - festzustellen, wann jemand an seinem Arbeitsplatz eintrifft. Dazu gehört auch das Wiedereintreffen nach einer Pause. Der Rückruf im Besetztfall erlaubt es, festzustellen, wie lange jemand telefoniert. Doch beide Leistungsmerkmale haben ihre Tücken: Der Rückruf im Freifall zeigt an, wann nach Abwesenheit das erste Gespräch beendet wurde, nicht das Ende der Abwesenheit selbst. Der Rückruf im Besetztfall zeigt an, wann nach dem laufenden Gespräch 15 Sekunden kein neues Gespräch begonnen wurde. Möglicherweise werden hier also Schlüsse gezogen, die falsch und für den Betroffenen nachteilig sind. Da er sich aber dazu nicht äußern kann, ist eine ungerechtfertigte Benachteiligung nicht ausgeschlossen. Hier ist die Aufklärung der Vorgesetzten über die tatsächliche Aussagekraft der so gewonnenen Informationen nötig.

Gerade bei größeren ISDN-Anlagen kommt eine weitere Gefahr und Mißbrauchsmöglichkeit hinzu: Es können Gesprächsprofile der Benutzer erstellt werden.¹³²

Die Anlagen speichern gesprächsbezogene Daten zu Abrechnungszwecken für einen gewissen Zeitraum. Wenn ein Unbefugter an diese Informationen herankommt, kann er sie auswerten und mißbrauchen: Aus ihnen lassen sich beispielsweise Geschäftsbeziehungen mit anderen Unternehmen ablesen. Daran könnten Konkurrenzunternehmen interessiert sein. Außerdem können Mitarbeiter erpreßbar werden, wenn ihr privates Kommunikationsverhalten am Firmenanschluß bekannt wird.

Die Gesprächsdaten sind also in jedem Fall besonders schützenswert. Der Schutz wird leider oft vernachlässigt, was aber ausschließlich im Verantwortungsbereich des Anlagenbetreibers liegt.

¹³² siehe Abschnitt 2.7.3

6 Verschlüsselung im ISDN

6.1 Einleitung

Die vorangegangenen Kapitel beschäftigten sich mit Schwachstellen des ISDN und möglichen Angriffen. Auf verschiedenen Ebenen und an verschiedenen Stellen wurden Angriffspunkte aufgezeigt. Die nun folgenden Kapitel behandeln Lösungsansätze für die gezeigten Probleme.

Dieses Kapitel befaßt sich mit der Verschlüsselung auf den verschiedenen Ebenen und untersucht bekannte Verschlüsselungsverfahren aus anderen Anwendungsbereichen, ob sie für die Anwendung im ISDN geeignet sind. Das nächste Kapitel befaßt sich mit Authentifizierungsverfahren und das übernächste untersucht, ob und wie der aus dem Internet bekannte Firewall-Mechanismus die Sicherheit im ISDN verbessern kann.

Man kann drei Sicherheitsanforderungen an Kommunikationssysteme unterscheiden:¹³³ Vertraulichkeit, Integrität und Verfügbarkeit.

Die Vertraulichkeit wird verletzt, wenn Andere von einer stattgefundenen Kommunikation oder sogar ihrem Inhalt Kenntnis erlangen. Hierunter fallen also beispielsweise Kommunikationsprofile und das Abhören oder Mitschneiden von Leitungen.

Die Integrität der übermittelten Nachrichten wird verletzt, wenn beim Empfänger nicht die Informationen ankommen, die der Absender an ihn übermittelt hat. Das kann sowohl eine vorgetäuschte Rufnummer als auch manipulierte Daten bei einer Fax- oder Datenübertragung sein.

Die Verfügbarkeit des Kommunikationssystems schließt die Verfügbarkeit der Leitungen und die Erreichbarkeit der Teilnehmer mit ein. Eine Reihe von Angriffen dagegen ist in den vorangegangenen Kapiteln beschrieben.

Zur Sicherung der Integrität und Vertraulichkeit der übermittelten Informationen können Verschlüsselung und Authentifizierung eingesetzt werden. Angriffe auf die Verfügbarkeit von Telekommunikationseinrichtungen sind oft mit der physikalischen Zerstörung von Einrichtungen und Leitungen verbunden. Dagegen schützen die hier vorgestellten Verfahren nicht.

6.2 Verschlüsselungsverfahren

Verschlüsseln heißt, einen Klartext mit Hilfe einer Rechenvorschrift und eines Schlüssels in einen Schlüsseltext zu überführen. Das macht nur Sinn, wenn es eine andere Rechenvorschrift gibt, die den Vorgang umkehrt.

Je nachdem, ob für das Entschlüsseln derselbe oder ein anderer Schlüssel verwendet wird, spricht man von symmetrischen und von asymmetrischen Verfahren.

6.2.1 Symmetrische und asymmetrische Kryptographie

Bei symmetrischen Kryptoverfahren wird derselbe Schlüssel sowohl zum Ver- als auch zum Entschlüsseln verwendet. Beide Kommunikationspartner müssen ihn kennen. Unabhängig davon, in welcher Richtung eine Nachricht gesendet wird, verwendet der jeweilige Absender diesen einen Schlüssel. Jeder Andere, der den Schlüssel kennt, kann die

¹³³ vgl. [sai97-1]

Kommunikation mitlesen und sogar gefälschte Nachrichten erzeugen und verschicken. Die Schlüsselhaber können echte von falschen Paketen nicht unterscheiden, vertrauen aber womöglich darauf, daß niemand ihren Schlüssel kennt und falsche Nachrichten erzeugen kann. Um die Echtheit tatsächlich beweisen zu können, müssen die Nachrichten zusätzlich digital unterschrieben werden.¹³⁴

Bei asymmetrischen Verfahren hat jeder Beteiligte zwei Schlüssel, einen öffentlichen und einen privaten. Wenn jemand eine Nachricht verschicken will, verschlüsselt er sie mit dem öffentlichen Schlüssel des Empfängers. Dieser kann sie mit Hilfe seines privaten Schlüssels lesen. Das Verfahren gewährleistet, daß man aus dem öffentlichen Schlüssel den privaten nicht mit vertretbarem Aufwand erhalten kann. Gängige Rechner benötigen bei sicheren Verfahren und heutigen Schlüssellängen Jahrhunderte um einen einzigen Schlüssel zu brechen.

Jeder, der den öffentlichen Schlüssel eines Beteiligten kennt, kann ihm eine Nachricht schicken. Der Empfänger kann die Gültigkeit nicht überprüfen, weiß das aber und wird sich deshalb ohne eine digitale Unterschrift oder vorangegangene Authentifizierung nicht darauf verlassen. Die digitale Unterschrift zu einer Nachricht kann man ebenfalls mit Hilfe eines solchen Verfahrens erzeugen.

Für ein symmetrisches Verfahren benötigt man bei n Benutzern $n*(n-1)/2$ verschiedene Schlüssel, damit jeder mit jedem kommunizieren kann. Dabei muß jeder Beteiligte alle $(n-1)$ Schlüssel kennen und geheimhalten, die er selbst mit Anderen vereinbart hat. Bei einer größeren Zahl von Benutzern wird die Schlüsselanzahl schnell unübersichtlich.

Für ein asymmetrisches Verfahren benötigt man nur doppelt so viele Schlüssel wie es Benutzer gibt. Jeder muß seinen eigenen privaten Schlüssel kennen und geheimhalten und kann die öffentlichen Schlüssel seiner Kommunikationspartner von Schlüsselservern abfragen.

Auch für die erstmalige Übermittlung der Schlüssel haben asymmetrische Verfahren Vorteile: Man kann Schlüsselserver verwenden. Neue Benutzer schicken ihren öffentlichen Schlüssel einfach an den Server. Jeder, der einem Anderen etwas übertragen will, erfragt beim Server den öffentlichen Schlüssel des Empfängers. Bei symmetrischen Verfahren muß ein neuer Benutzer zunächst mit jedem seiner zukünftigen Kommunikationspartner einen eigenen Schlüssel vereinbaren. Meist steht dazu nur ein unsicherer Kanal zur Verfügung¹³⁵, so daß die Schlüssel selbst verschlüsselt übertragen werden müssen. Das klingt zunächst paradox, läßt sich mit Hilfe spezieller Verfahren aber lösen.¹³⁶

Wenn ein geheimer Schlüssel einmal bekannt geworden ist, muß er als ungültig erklärt werden. Das ist bei asymmetrischen Verfahren schwieriger als bei symmetrischen: Der betroffene Benutzer teilt dem Schlüsselserver den ungültigen Schlüssel zusammen mit seinem neuen öffentlichen Schlüssel mit. Der beantwortet alle Anfragen mit dem neuen Schlüssel. Dennoch kann es Benutzer geben, die nicht beim Schlüsselserver anfragen, weil sie den (inzwischen ungültigen) öffentlichen Schlüssel des Empfängers kennen.¹³⁷ Bei einem symmetrischen Verfahren muß dagegen nur zwischen den beiden Betroffenen, deren Schlüssel bekannt wurde, ein neuer vereinbart werden.

¹³⁴ siehe dazu z.B. [sch96-1], Kapitel 20; mehr dazu im nächsten Kapitel

¹³⁵ denn über die Telefonleitung kann ja (noch) nicht verschlüsselt kommuniziert werden.

¹³⁶ siehe [sch96-1] Kapitel 8

¹³⁷ Eine Lösung für dieses Problem sind Gültigkeitsintervalle

In puncto Geschwindigkeit haben die symmetrischen Verfahren die Nase vorne. Sie sind um Faktoren schneller als die asymmetrischen. In der Praxis verwendet man deshalb eine Mischung aus beiden:

Zunächst wird mit Hilfe eines asymmetrischen Verfahrens ein sogenannter Sitzungsschlüssel vereinbart. Das ist ein symmetrischer Schlüssel, der zufällig erzeugt und nur für diese eine Kommunikation verwendet wird. Er wird mit einem asymmetrischen Verfahren an alle beteiligten Kommunikationspartner übermittelt. Ab dann wird mit Hilfe eines symmetrischen Verfahrens weiter gearbeitet. So ist auch eine vertrauliche Kommunikation ganzer Gruppen möglich.

6.2.2 Blockchiffren

Beim Einsatz von Blockchiffren wird die zu verschlüsselnde Nachricht in Blöcke fester Länge (meist 64 Bit) geteilt und diese werden verschlüsselt. Es gibt verschiedene Modi: Den electronic-codebook-Modus (ECB), den cipher-block-chaining-Modus (CBC) und den cipher-feedback-Modus (CFB). Beim ECB wird derselbe Klartextblock mit dem selben Schlüssel immer zum selben Schlüsseltext codiert, beim CBC hängt das Verschlüsselungsergebnis auch von den vorangegangenen Blöcken ab.

Daneben gibt es noch eine Reihe von Varianten, auf die ich hier nicht näher eingehe.¹³⁸

6.2.3 Stromchiffren

Eine Stromchiffre verschlüsselt bitweise und das Ergebnis hängt ja nach dem verwendeten Verfahren nicht nur vom Schlüssel sondern auch von der vorangegangenen Nachricht ab. Ein und die selbe Nachricht wird also in verschiedenen Zusammenhängen trotz gleichen Schlüssels zu unterschiedlichen Schlüsseltexten verarbeitet.

Dazu verfügen Sender und Empfänger über Zufallsgeneratoren, die zu jedem Schlüssel einen anderen, festen Bitstrom generieren. Der Sender verknüpft den Klartext XOR mit dem erzeugten Schlüsselstrom. Der Empfänger erhält nach Eingabe des selben Schlüssels den Schlüsselstrom, den auch der Sender verwendet hat. Er verknüpft die verschlüsselte Nachricht mit diesem Strom und erhält den Klartext.

Bei den Stromchiffren gibt es selbstsynchronisierende (ciphertext auto key, CTAK) und synchrone (key auto key, KAK) Varianten.

Bei den selbstsynchronisierenden hängt jedes Bit des Schlüsselstroms von einer festen Anzahl vorangegangener Bits ab. Der Schlüsselstromgenerator synchronisiert sich von selbst, wenn er diese Anzahl Bits empfangen hat. Man stellt einer so verschlüsselten Nachricht einfach einen header dieser Länge voran. Nachdem ihn der Empfänger mit Hilfe seines Schlüssels entschlüsselt hat, sind beide Schlüsselstrom-Generatoren synchronisiert.

Bei KAK müssen die Schlüsselstrom-Generatoren des Senders und des Empfängers auf eine andere Weise synchronisiert werden. Das Verfahren arbeitet nur korrekt, solange sie synchron sind. Dafür ist diese Variante immun gegen die Fehlerfortpflanzung.

6.3 Verschlüsselungsmöglichkeiten im ISDN

Man unterscheidet die abschnittsweise (link-by-link-) und die Ende-zu-Ende (end-to-end-) Verschlüsselung von Kommunikationskanälen.¹³⁹ Beide haben Vor- und Nachteile:

¹³⁸ Sie sind bei [sch96-1] nachzulesen.

6.3.1 Abschnittsweise Verschlüsselung

Bei der abschnittswisen Verschlüsselung werden die Daten jeweils zwischen zwei Stationen auf dem Weg vom Sender zum Empfänger neu verschlüsselt. Das hat den Vorteil, daß die Stationen nur jeweils die Schlüssel ihrer unmittelbaren Nachbarn kennen müssen, aber den Nachteil, daß durch die häufige Ver- und Entschlüsselung eine Verzögerung auftritt. Außerdem ist beim Empfänger nicht nachzuvollziehen, ob die Daten in einem der Knoten manipuliert wurden. Dieses Verfahren schließt nur die Manipulation der Daten auf den einzelnen Teilstrecken zwischen den Knoten aus.

Es eignet sich besonders für die Absicherung der Steuerdaten im ISDN. Denn sie müssen ohnehin in jedem Knoten ausgewertet werden. Wenn der Netzbetreiber die Sicherheit seiner Knoten gewährleisten kann, ist so eine sichere Steuerung der Kommunikationsverbindungen möglich.

Für die Verschlüsselung der Nutzkanäle eignet es sich aufgrund der beschriebenen Nachteile nicht.

6.3.2 Ende-zu-Ende-Verschlüsselung

Bei der Ende-zu-Ende-Verschlüsselung werden die Daten beim Absender verschlüsselt, durch das Netz über mehrere Knoten transportiert und erst beim Empfänger wieder entschlüsselt. Die Daten können unterwegs nicht manipuliert werden, weil sie während der Übertragung auch in den Knoten nie unverschlüsselt vorliegen. Dieses Verfahren ist besonders gut für die Verschlüsselung der Nutzkanäle (B-Kanäle) geeignet. Sie müssen im Laufe der Übertragung nicht ausgewertet werden, da die Steuerinformationen in den D- und ZGS-7-Kanälen enthalten sind und Nutzkanäle transparent über alle dazwischenliegenden Vermittlungsstellen durchgeschaltet werden.

6.3.3 Verschlüsselung der B-Kanäle

In den B-Kanälen werden die eigentlichen Nutzdaten zwischen den beiden verbundenen Anschlüssen übertragen. Die Vermittlungsstellen transportieren 64kBit/sec in beiden Richtungen, ob Daten enthalten sind oder nicht und unabhängig vom Inhalt.

Das macht die Verschlüsselung im B-Kanal relativ leicht. Sie ist vom Netz unabhängig; Die beiden Kommunikationspartner können individuell vereinbaren, ob sie überhaupt verschlüsseln und wenn ja nach welchem Verfahren. Dazu brauchen sie gegebenenfalls noch einen geeigneten Schlüssel. Sie müssen sich dabei an keine Standards halten. Im Extremfall können sie ein eigenes Verschlüsselungsverfahren entwickeln und verwenden.

Sie benötigen aber entsprechende Endgeräte, die die Ver- und Entschlüsselung für sie durchführen. Beim Telefonieren müssen also die Telefone an beiden Enden der Leitung zueinander kompatibel sein. Das ist die Schattenseite der Freiheit durch fehlende Standards: Das Telefon eines Teilnehmers muß alle Verschlüsselungsverfahren der Endgeräte aller anderen Teilnehmer beherrschen, mit denen er verschlüsselt telefonieren will.

Das ist für die Kommunikation innerhalb einer bestimmten Gruppe von Teilnehmern kein Problem: Sie müssen sich nur auf ein Verfahren einigen. Jeder Teilnehmer, der der Gruppe beitreten will, muß sich dem verwendeten Verfahren anpassen. Außenstehende Teilnehmer oder solche aus anderen Gruppen können nicht sicher mit den Gruppenmitgliedern oder miteinander kommunizieren. Dazu müßte die Verschlüsselung in den Euro-

¹³⁹ vgl. [sch96-1] Abschnitt 10.3

ISDN-Standard aufgenommen und ein einheitliches Verfahren in alle Endgeräte implementiert werden.

Viel leichter ist das Verschlüsseln beim Telefonieren oder Datenaustausch mit Hilfe von Computern. Es ist ein Trend hin zur computergestützten Telefonie zu erkennen. Dabei wird ein Telefonhörer oder eine Kopfhörer-Mikrofon-Kombination an einen Computer angeschlossen, der mit einer ISDN-Karte ausgestattet ist. Die Bedienung erfolgt mit Hilfe spezieller Software. Sie kann auch die Verschlüsselung der zu übertragenden Daten oder der Sprache übernehmen. Dabei läßt sich die Software erheblich leichter an andere Verschlüsselungsverfahren anpassen als Hardware.

Das oben Gesagte gilt auch für die zahlreichen anderen ISDN-Dienste. Sie alle übertragen letztendlich Daten, die von speziellen Endgeräten interpretiert und gegebenenfalls in wahrnehmbare Reize umgewandelt werden. Wenn diese Endgeräte selbst keine Verschlüsselung unterstützen, können Verschlüsselungsgeräte zwischengeschaltet werden. Sie arbeiten unabhängig von Endgeräten und ver- bzw. entschlüsseln die 64kBit/sec-Daten eines oder mehrerer Endgeräte in Echtzeit. Die Endgeräte bemerken den Vorgang nicht.

6.3.4 Verschlüsselung des D-Kanals

Auch der Inhalt des D-Kanals läßt sich verschlüsseln. Dadurch kann man die Daten, die eine Verbindung steuern, vor Manipulation und Abhören schützen.

Das D-Kanal-Protokoll ist international genormt. Alle Vermittlungsstellen und alle Endgeräte verstehen und verwenden es. Eine generelle Einführung von Verschlüsselung im D-Kanal erfordert die Ergänzung und Anpassung des D-Kanal-Protokolls. Das zieht Änderungen in allen Teilnehmervermittlungsstellen und bei allen eingesetzten Endgeräten nach sich. Die Vermittlungsstellen, ISDN-TK-Anlagen und moderne Telefone sind softwareprogrammiert und lassen sich deshalb mit einer Softwareänderung an neue Standards anpassen. Für andere Geräte kann man einen Kompatibilitätsmodus ohne Verschlüsselung, aber auch ohne Sicherheit vorsehen.

Die Verschlüsselung der Daten im D-Kanal aus Richtung des Kunden schützt ihn vor Mißbrauch seiner Telefonleitung. Zusammen mit der Authentifizierung des Endgeräts¹⁴⁰ stellt sie sicher, daß Verbindungen nur von einem Endgerät des Kunden aufgebaut werden können.

Außerdem schützt sie den Netzbetreiber, weil Manipulationsversuche an der Vermittlungsstelle eindeutig einem Kunden zugeordnet werden können. Ein Angreifer, der sich auf die Teilnehmeranschlußleitung aufgeklemt haben könnte, scheidet aus.

Die Verschlüsselung des D-Kanals in umgekehrter Richtung zusammen mit der Authentifizierung der Vermittlungsstelle schützt den Kunden vor Angriffen auf seine Endgeräte. Zumindest solange sie nicht aus der Vermittlungsstelle heraus sondern durch Aufklemen auf den D-Kanal¹⁴¹ erfolgen.

Außerdem kann so niemand durch Abhören des D-Kanals ein Kommunikationsprofil¹⁴² erstellen.

¹⁴⁰ siehe Abschnitt 7.3.2

¹⁴¹ siehe Abschnitt 5.2.5

¹⁴² siehe Abschnitt 2.7.3

6.3.5 Verschlüsselung der ZGS-7-Kanäle

Auch auf das Zeichengabe-7-Netz (ZGS-7) sind zahlreiche Angriffe möglich. Sie sind in Kapitel 4 beschrieben. Ein Teil dieser Angriffe läßt sich ausschließen, wenn die Daten zwischen den Netzknoten verschlüsselt übertragen werden.

Sie können dann nicht mehr abgehört werden. Damit ist es nicht mehr möglich, Kommunikationsprofile von Teilnehmern zu erstellen. Außerdem können die übertragenen Steuerdaten nicht mehr verändert werden. Das vermeidet die Angriffe gegen eine Vermittlungsstelle über das ZGS-7. Es sei denn, eine Vermittlungsstelle wurde auf anderem Wege bereits manipuliert und greift nun ihrerseits andere Vermittlungsstellen an. Dagegen hilft auch die Verschlüsselung nicht.

Es wird einem Angreifer so auch nicht mehr gelingen, zusätzliche Datenpakete ins ZGS-7 einzuschleusen und zu einem Ziel seiner Wahl transportieren zu lassen.

Das ZGS-7 transportiert eine Mischung aus Ende-zu-Ende und abschnittsweise ausgewerteten Paketen. Ende-zu-Ende Pakete werden erst in der Zielvermittlungsstelle ausgewertet. Dazu gehören beispielsweise die Rufnummer des Anrufenden, die Information, ob diese angezeigt werden darf und eventuelle User-to-User-Signalling-Pakete. Die abschnittsweise ausgewerteten Pakete dienen der Steuerung der eigentlichen Nutzkanalverbindung. Sie müssen in jedem Knoten auf dem Weg von der Ursprungs- zur Zielvermittlungsstelle vorliegen. Deshalb können sie nicht Ende-zu-Ende verschlüsselt werden.

Doch auch die Ende-zu-Ende-Pakete werden in den unteren Schichten des ZGS-7 abschnittsweise übertragen. Sie enthalten neben der Zieladresse auch die Adresse des nächsten Knotens auf dem Weg zum Ziel. Diese wird in jedem Knoten durch die nächste ersetzt. Zumindest diese Teile können also auch bei Ende-zu-Ende-Paketen nur abschnittsweise verschlüsselt werden. Näheres dazu später.

6.3.6 Verschlüsselung innerhalb der ISDN-TK-Anlagen

Beim Betrieb einer ISDN-TK-Anlage an einem Anschluß bieten sich eine Reihe zusätzlicher Angriffspunkte. Im Prinzip verhalten sich TK-Anlage und Benutzer-Endgeräte zueinander wie Vermittlungsstelle und Endgeräte ohne TK-Anlage. Aber eine TK-Anlage ist leichter zu manipulieren als eine Vermittlungsstelle. Deshalb macht es auch Sinn, innerhalb der TK-Anlage zu verschlüsseln und zu authentifizieren.

Dabei muß man unterscheiden zwischen analogen und digitalen Nebenstellen:

Bei ISDN-Anlagen mit analogen Endgeräten übernimmt die Anlage die Umsetzung zwischen den beiden Technologien. Auf der Teilnehmeranschlußleitung werden die Steuerdaten gemeinsam mit den Nutzdaten „inband“ übermittelt.

Hier kann man also nur entweder alles oder nichts verschlüsseln. Man muß sich bei der Verschlüsselung nicht an Standards halten, sondern kann eigene Protokolle verwenden. Denn die Anlage muß ohnehin wieder entschlüsseln, zwischen Steuer- und Nutzdaten unterscheiden und gegebenenfalls in Richtung der Vermittlungsstelle neu verschlüsseln.

Eine Alternative ist die Verschlüsselung im oder bereits vor dem Endgerät, beispielsweise in einem Computer mit einem Modem. Die bereits verschlüsselten Daten werden dann zusammen mit den unverschlüsselten Steuerdaten zur Anlage übertragen. Diese trennt die Steuerdaten von den Nutzdaten. Die Steuerdaten werden interpretiert, die Nutzdaten auf einen B-Kanal weitergeleitet. Die Anlage kann dabei nicht erkennen, daß die Nutzdaten verschlüsselt sind.

Bei ISDN-Anlagen mit digitalen Nebenstellen bildet die Anlage eine digitale Vermittlungsstelle nach. Hier gilt also in bezug auf Verschlüsselung im Prinzip alles, was für die Vermittlungsstelle auch gilt.

Zwischen Benutzer-Endgerät und Anlage werden die Nutz- und die Steuerdaten in getrennten Kanälen auf einer Leitung übermittelt. Das bietet die Möglichkeit Nutz- und Steuerkanäle getrennt und unabhängig voneinander zu verschlüsseln oder auch nicht. Abstrakt betrachtet ist in diesem Fall die ISDN-TK-Anlage aus Sicht des B-Kanals nur eine weitere Vermittlungsstelle zwischen den beiden Kommunikationspartnern. Für den D-Kanal stimmt das so nicht, denn er ist jetzt dreimal vorhanden: Zwischen dem Endgerät und der Anlage, zwischen der Anlage und der Vermittlungsstelle und zwischen der Zielvermittlungsstelle und dem Endgerät am anderen Ende der Kommunikationsbeziehung.¹⁴³

In jedem Fall läßt sich aber bereits innerhalb der Anlage verschlüsseln: Die B-Kanäle werden ohnehin transparent durchgereicht. Der Inhalt des D-Kanals muß in der Anlage wieder entschlüsselt werden, damit er ausgewertet werden kann. Nach Außen hin kann sie ihn mit ihrem eigenen Schlüssel in Richtung der Vermittlungsstelle wieder verschlüsseln.

Auch bei ankommenden Gesprächen wird der D-Kanal in der ISDN-Anlage entschlüsselt und ausgewertet. Mit Hilfe der so gewonnenen Steuerungsinformation wird der Inhalt des B-Kanals transparent an das richtige Endgerät weitergeleitet.

6.4 Wer will überhaupt verschlüsseln?

Bei den Überlegungen zur Verschlüsselung im ISDN muß man auch immer die unterschiedlichen Interessen der Beteiligten betrachten. Dazu gehören neben den Benutzern der Endgeräte auch deren Betreiber¹⁴⁴ und die Netzbetreiber. Man darf auch nicht die Interessen der staatlichen Stellen wie Polizei, Verfassungsschutz und Geheimdienste vergessen.

Die Benutzer wollen, daß der Inhalt ihrer Gespräche und Datenverbindungen nicht abgehört oder manipuliert werden kann. Außerdem wollen sie nicht, daß ihre Leitungen durch Andere genutzt werden können. Und sie wollen im Allgemeinen nicht, daß Kommunikationsprofile über sie erstellt werden.

Die Betreiber von ISDN-TK-Anlagen wollen außerdem nicht, daß Angreifer von innen oder von außen an der Konfiguration der Anlage manipulieren können.

Die Netzbetreiber wollen, daß ihre Vermittlungsstellen und Verbindungswege sicher sind. Denn Sicherheit wird ein wesentliches Verkaufsargument konkurrierender Netzbetreiber mit vergleichbarem Leistungsspektrum. Sie wollen außerdem nicht, daß auf ihre Kosten kommuniziert wird oder Daten in einem ihrer Netze übertragen werden. Und wenn Manipulationen vorkommen, sollen sie eindeutig dem Verursacher zugeordnet werden können. Am Besten auch beweisbar.

Diesen Sicherheitsinteressen stehen die Interessen der staatlichen Stellen gegenüber. Sie wollen alle übertragenen Nutzinformationen abhören können. Dazu gehören die Informationen, wer wann mit wem kommuniziert hat und auch die Inhalte der Gespräche oder

¹⁴³ Falls dort auch eine ISDN-Anlage mit digitalen Endgeräten installiert ist, gibt es sogar vier D-Kanal-Abschnitte

¹⁴⁴ bei privaten Anschlüssen ist der Benutzer auch der Betreiber

die übertragenen Daten. Sie werden sich deshalb immer gegen eine Verschlüsselung der Nutz- und Steuerkanäle wehren. Oder sie fordern speziell für sie eingebaute Hintertürchen wie beim amerikanischen Clipper-Chip.

In Frankreich ist beispielsweise Verschlüsselung jeglicher Art verboten. Deshalb dürfte es schwer sein, Verschlüsselung als Pflichtelement in den Euro-ISDN-Standard aufzunehmen.

6.5 Besondere Anforderungen des ISDN an die Verschlüsselung

In einem Telekommunikationsnetz wie dem ISDN bestehen besondere Anforderungen an kryptographische Verfahren. Sie entstehen aus der historisch gewachsenen Struktur und aus besonderen Eigenschaften eines solchen Netzes. Im Folgenden werden einzelne Eigenschaften und die sich ergebenden Anforderungen beschrieben:

6.5.1 Sehr große Teilnehmerzahl

Allein in Deutschland gibt es 35 Millionen Telefonanschlüsse. Früher oder später werden sie alle digitalisiert sein. Weltweit dürften es mehrere hundert Millionen Anschlüsse sein. Sie sind an Netzen in ganz unterschiedlicher Technik angeschlossen. Dennoch wollen alle Teilnehmer mit allen anderen Teilnehmern weltweit uneingeschränkt kommunizieren können. Deshalb muß es Netzübergänge geben.

Die eingesetzten Verschlüsselungsverfahren müssen also für eine große Zahl von Teilnehmern in jeder beliebigen Kombination geeignet sein. Bei der Kommunikation über Netzgrenzen hinweg können sie zwischen dem ISDN-Teilnehmer und dem Netzübergang verschlüsseln. Damit ist zumindest einem Angriff aus dem ISDN heraus vorgebeugt. Nach dem Gesetz des schwächsten Glieds¹⁴⁵ ist diese Kommunikation aber nicht sicher.

Außerdem scheiden alle Verfahren aus, bei denen vorab über einen sicheren Kanal Schlüssel ausgetauscht werden müssen. Dazu müßten die Teilnehmer erst einmal per Post oder in einem persönlichen Treffen Schlüssel für die spätere Kommunikation vereinbaren. Das ist unpraktikabel.

6.5.2 Verzögerungen

Kommunikation über das ISDN geschieht in Echtzeit. Sowohl beim Verbindungsaufbau als auch während der Verbindung dürfen deshalb keine zu großen Verzögerungen auftreten.

Dabei wird die Verzögerung beim Verbindungsaufbau durch die Verschlüsselung der Steuerdaten in den D-Kanälen und im ZGS-7 bestimmt. Mit der Einführung des ISDN wurden die Verbindungsaufbauzeiten von mehreren Sekunden auf 0,8 bis 1,7 Sekunden gesenkt.¹⁴⁶ Diesen Fortschritt will man nicht wieder aufgeben. Das verwendete Verfahren muß sich also effizient in Hardware implementieren lassen.

Während der Verbindung würde sich eine zu große Verzögerung noch störender auswirken: Bei Telefongesprächen entstehen Pausen wie man sie von Überseegesprächen her kennt, bei Datenübertragungen kann es zum Abbruch der Verbindung kommen, wenn die Quittung für ein Paket zu lange braucht. Hier sind also effizient in Software implementierbare Verfahren wichtig.

¹⁴⁵ „Eine Kette ist nur so stark wie ihr schwächstes Glied.“

¹⁴⁶ je nach dem wie viele Vermittlungsstellen beteiligt sind.

6.5.3 Schlüssellänge

Für die genannten Verzögerungen spielt auch die Länge der verwendeten Schlüssel eine Rolle: Hier stehen sich Sicherheit und Effizienz gegenüber. Je länger der gewählte Schlüssel ist, desto schwieriger ist er zu knacken. Aber je kürzer er ist, desto schneller arbeitet die Verschlüsselung. Man muß also einen Kompromiß finden, der bestmögliche Sicherheit bei gerade noch akzeptabler Verzögerung bietet.

6.5.4 Konferenzschaltungen

Ein Ziel der Verschlüsselung im B-Kanal ist es, das Abhören zu vermeiden. Nur die beiden Kommunikationspartner sollen das Gesprochene oder die Daten verstehen können. Daraus ergibt sich aber ein Problem bei den Konferenzschaltungen. Hier will man ja gerade mehr als zwei Kommunikationspartner miteinander verbinden. Dabei macht die Konferenzschaltung nur bei Telefongesprächen, nicht aber bei der Datenübertragung Sinn.

Bei einer Dreierkonferenz¹⁴⁷ wird der Inhalt von jeweils zwei B-Kanälen gemischt und zum dritten Gesprächspartner übertragen.

Das Verschlüsselungsverfahren muß deshalb geeignet sein, auch solche gemischten verschlüsselte Datenströme richtig zu entschlüsseln. Dem Autor sind keine am Markt angebotenen Verschlüsselungsgeräte bekannt, die Konferenzschaltungen unterstützen

6.5.5 Länge des Schlüsseltextes

Bei der Verschlüsselung der Datenpakete des D-Kanals und des ZGS-7 möchte man möglichst keine Protokolländerungen vornehmen müssen. Die verschlüsselten Pakete müssen deshalb genauso lang sein wie die unverschlüsselten.

Noch wichtiger ist diese Forderung¹⁴⁸ bei der Verschlüsselung der Nutzkanäle. Ein B-Kanal überträgt 64kbit/sec transparent von einem Ende einer Verbindung zum anderen. Hierbei darf der verschlüsselte Text auf gar keinen Fall größer sein als der Klartext. Andernfalls treten stetig wachsende Verzögerungen auf und es kommt zu Datenverlust.

Die wenigen Verschlüsselungsverfahren, die diese Forderung nicht erfüllen, scheiden deshalb für den Einsatz im ISDN aus.

6.5.6 Gültigkeitsdauer

Zwei Kommunikationspartner können über Jahre hinweg ihre Gespräche mit dem selben Schlüssel vor neugierigen Ohren schützen. Sobald der Schlüssel aber kompromittiert wird, liegen alle Gespräche offen. Mit Hilfe eines lange gültigen Schlüssels kann für jede Verbindung ein neuer Schlüssel¹⁴⁹ vereinbart werden.¹⁵⁰ Mit ihm werden die eigentlichen Nutzdaten verschlüsselt.

Da der lange gültige Schlüssel immer nur für wenige Bytes verwendet wird, ist er nicht so leicht zu brechen. Und die jeweils vereinbarten Sitzungsschlüssel werden zufällig erzeugt, haben nichts miteinander zu tun und werden auch immer nur für eine Verbindung

¹⁴⁷ Eine größere Konferenz mit bis zu 10 Teilnehmern funktioniert ähnlich

¹⁴⁸ siehe [sch96-1] Seite 223

¹⁴⁹ ein sogenannter Sitzungsschlüssel, „session key“

¹⁵⁰ vgl. [sch96-1] Seite 215

benutzt. So entsteht mit keinem Schlüssel eine Datenmenge kritischer Größe, die ihn leicht knacken ließe.

6.6 Eignung/Anpassung bekannter Verfahren

Aufbauend auf den oben genannten Anforderungen und Verschlüsselungsmöglichkeiten werden jetzt konkrete Einsatzgebiete und geeignete Verfahren untersucht. An einigen Stellen sind Einschränkungen oder Anpassungen nötig.

6.6.1 Abschnittsweise oder Ende-zu-Ende-Verschlüsselung?

Die Steuerdaten einer Telekommunikationsbeziehung werden in allen Zwischenstationen ausgewertet. Diese Zwischenstationen sind die Teilnehmer-Endgeräte, eine eventuell vorhandene TK-Anlage, die Ursprungsvermittlungsstelle, gegebenenfalls mehrere Durchgangsvermittlungsstellen, die Zielvermittlungsstelle und die Endeinrichtungen beim Angerufenen. Sie müssen deshalb abschnittsweise verschlüsselt werden.

Eine Ausnahme stellen die Pakete der Steuerdaten dar, die transparent bis zum Zielteilnehmer befördert werden. Sie enthalten die Zieladresse und die Adresse der nächsten Zwischenstation auf dem Weg zum Ziel. In den Zwischenstationen werden sie nicht bis in die oberste Schicht durchgereicht sondern sie erhalten lediglich die Zieladresse der nächsten Zwischenstation. Dazu muß der Teil des Pakets entschlüsselt werden, der die Adressen enthält. Der Rest kann verschlüsselt bleiben. Hier bietet es sich an, zwei verschiedene Schlüssel zu verwenden:

Der erste Teil mit den Adressen wird mit dem Schlüssel der nächsten Zwischenstation verschlüsselt, der transparent zu übertragende Teil wird gleich mit dem Schlüssel des Ziels verschlüsselt. Hier liegt also eine Mischform von abschnittsweiser und Ende-zu-Ende-Verschlüsselung vor.

Die Nutzdaten hingegen sollen in den Zwischenstationen gar nicht ausgewertet werden können. Hier bietet sich die Ende-zu-Ende-Verschlüsselung an.

6.6.2 Symmetrisches oder asymmetrisches Verfahren?

Wegen der großen Anzahl der Teilnehmer im weltweiten Telekommunikationsverbund und wegen der leichteren Schlüsselverwaltung sind asymmetrische Verfahren im Vorteil. Dem gegenüber steht der klare Geschwindigkeitsvorteil der symmetrischen Verschlüsselung.

Die ideale Lösung für die Ende-zu-Ende-Verschlüsselung stellt deshalb eine Mischform dar, wie sie beispielsweise auch das bekannte Programm `pgp`¹⁵¹ verwendet: Zu Beginn der Kommunikation wird mit Hilfe eines asymmetrischen Verfahrens ein Sitzungsschlüssel vereinbart. Mit diesem wird die eigentliche Kommunikation symmetrisch verschlüsselt.

Damit dieses Verfahren funktionieren kann, muß eine Hierarchie von Schlüsselservern installiert werden. Sie stellen einen Engpaß dar, so daß für eine reibungslose Kommunikation eine ausreichende Anzahl von Servern bereit gestellt werden muß. Auf der anderen Seite sind sie ein lohnendes Angriffsziel, denn sie haben alle Teilnehmerschlüssel und alle Teilnehmer vertrauen ihnen. Deshalb müssen sie besonders gut geschützt werden.

¹⁵¹ pretty good privacy, ein kostenloses Programm zur Verschlüsselung und Signatur von e-mails etc.

Für die abschnittsweise Verschlüsselung der Steuerdaten eignet sich ein symmetrisches Verfahren mit beschränkter Schlüssellebensdauer am besten, da hier jeder Knoten nur mit seinen unmittelbaren Nachbarn kommuniziert, immer nur kurze Pakete ausgetauscht werden und im Prinzip eine ständige Kommunikationsverbindung besteht. Hier ist ein asymmetrisches Verfahren zu langsam.

6.6.3 Block- oder Stromchiffre?

Für den Einsatz im ISDN eignen sich Block- und Stromchiffren gleichermaßen, wenn man einige Randbedingungen beachtet:

Auf einer niedrigen Ebene des 7-Schichten-Protokolls werden in den Nutz- und Steuerkanälen ohnehin ständig die maximal möglichen 9.6 bzw. 64 kBit/sec übertragen. Wenn man hier die Verschlüsselung implementiert, sind Block- und Stromchiffren gleichwertig. Wenn man aber höhere Ebenen betrachtet, so werden Daten bereits dann übertragen, wenn sie anfallen. Hier sind Stromchiffren den Blockchiffren überlegen.

Beim Einsatz von Blockchiffren muß man einen Modus verwenden, bei dem der Schlüsseltext nicht nur von den aktuellen Daten sondern auch von den vorangegangenen verschlüsselten Blöcken abhängt. Damit schützt man sich vor block-replay-Angriffen. Dabei werden gesendete Blöcke von einem Angreifer zwischengespeichert und zu einem späteren Zeitpunkt erneut eingespielt. Er kann dann zwar den Inhalt der Blöcke nicht verändern, aber unter Umständen reicht schon die Wiederholung für einen erfolgreichen Angriff aus.

7 Authentifizierung im ISDN

7.1 Einleitung

Mit der Verschlüsselung einer Nachricht stellt man sicher, daß sie nicht abgehört werden kann. Bei der Authentifizierung muß ein Kommunikationspartner dem anderen seine Identität beweisen. Kommunikationspartner können dabei sowohl Personen als auch Computer, Telefone, sonstige Endgeräte, Vermittlungsstellen oder Netzknoten sein. In diesem Kapitel werden zunächst bekannte Authentifizierungsverfahren vorgestellt. Anschließend werden die Authentifizierungsmöglichkeiten an den verschiedenen Stellen im ISDN systematisch untersucht. Daraus ergeben sich besondere Anforderungen des ISDN an die Authentifizierung, die Anpassungen nötig machen. Beides steht am Ende des Kapitels.

7.2 Bekannte Authentifizierungsverfahren

Zum Identitätsbeweis verwendet man ein Geheimnis, das beide Kommunikationspartner kennen (secret-key-Authentifizierung) oder eines, das nur einer der Kommunikationspartner kennt. Der andere muß dann eine Möglichkeit haben, es nachzuprüfen, ohne daß es verraten werden muß (public-key-Authentifizierung, zero-knowledge-proof).

Die wohl bekannteste Art, seine Identität gegenüber einer elektronischen Anlage zu beweisen, stellt das Paßwort dar. Es kann zusammen mit der Benutzererkennung eingegeben werden wie bei Rechnern oder zusammen mit einer Chip- oder Magnetkarte verwendet werden wie zum Beispiel die PIN bei Scheckkarten. Beide Formen sind secret-key-Authentifizierung.

Viele Authentifizierungsverfahren sind auch geeignet, gleichzeitig einen Sitzungsschlüssel zur Verschlüsselung der anschließenden Kommunikation zu vereinbaren.¹⁵²

7.2.1 Secret-key-Authentifizierung

Bei dieser Form kennen beide Seiten ein gemeinsames Geheimnis. Um die Echtheit zu beweisen, übermittelt die eine Seite der anderen das Geheimnis. Das setzt einen abhörsicheren Kanal voraus. Ein Anwendungsbeispiel ist das Anmelden per Benutzername und Paßwort an einem Computer. Dieser verfügt über eine Datei mit allen Benutzernamen/Paßwort-Kombinationen der registrierten Benutzer. Das macht ihn zur zentralen Schwachstelle des Systems. Wer die Liste in seine Gewalt bringt, kann unbemerkt die Identität aller darin gespeicherter Benutzer annehmen. Deshalb wird nicht das Paßwort selbst sondern ein Hashwert des Paßworts gespeichert. Wenn ein Benutzer sich anmeldet, wird das eingegebene Paßwort gehasht und dieser Hashwert mit dem gespeicherten verglichen.

Jetzt könnte man meinen, auch das Problem des sicheren Kanals lösen zu können, indem man das Paßwort vor der Übertragung bereits hasht. Das funktioniert aber nicht. Wenn bereits der Hashwert des Paßworts übertragen wird, hat man ein Verfahren, das dem Übertragen des Paßworts im Klartext gleichkommt: Wer die Liste der Hashwerte hat, kann betrügen.

¹⁵² vgl. [sch96-1] Abschnitt 3.3

Ein weiteres Problem bei der secret-key-Authentifizierung ist die Gefahr des sogenannten Wörterbuchangriffs: Ein Angreifer besorgt sich die Datei mit den Benutzernamen und den gehashten Paßwörtern. Das verwendete Hashverfahren ist in der Regel öffentlich bekannt. Anschließend hasht er alle Wörter eines Wörterbuches und vergleicht die Ergebnisse mit jedem Hashwert in der Datei. Stimmen zwei überein, kennt er das Paßwort des zugehörigen Benutzers. Dieses Verfahren ist sehr erfolgversprechend. Es gibt einige Erweiterungen, um die Sicherheit etwas zu erhöhen.¹⁵³

7.2.2 Public-key-Authentifizierung

Sicherer ist die Authentifizierung mit einem public-key-Verfahren. Hier muß das Geheimnis weder übertragen werden noch muß es (oder sein Hashwert) zentral gespeichert werden. Ein solches Verfahren arbeitet ähnlich wie asymmetrische Verschlüsselung: Jeder Benutzer hat einen geheimen Schlüssel. Damit „unterschreibt“ er digital eine Nachricht (beispielsweise eine Zufallszahl, einen Zeitstempel oder ähnliches). Der Empfänger der Nachricht kann in einem öffentlichen Verzeichnis den öffentlichen Schlüssel des Absenders nachsehen und mit seiner Hilfe überprüfen, daß sie mit dem dazugehörigen geheimen Schlüssel erzeugt wurde.

Das Verfahren basiert also wie die symmetrische Authentifizierung darauf, ein Geheimnis zu kennen. Es hat aber die Vorteile, daß das Geheimnis nie übertragen werden muß und daß die Menge der benötigten Schlüssel überschaubar bleibt und trotzdem jeder mit jedem kommunizieren kann. Man kann es also auch dann einsetzen, wenn kein sicherer Kanal zur Verfügung steht.

Es hat den Nachteil, daß es eine zentrale Instanz benötigt, der alle Kommunikationspartner vertrauen müssen: Den Server mit den öffentlichen Schlüsseln aller Benutzer. Er ist die zentrale Schwachstelle des Systems und muß besonders gegen Angriffe gesichert werden.

7.2.3 Authentifizierung mit Einmalpaßwörtern

Mit Hilfe einer Einwegfunktion kann man eine Liste von Paßwörtern vorausberechnen: Man nimmt einen beliebigen Startwert und wendet die Einwegfunktion darauf an. Das Ergebnis speichert man ab und wendet darauf wieder die Einwegfunktion an. Damit lassen sich beliebig viele Paßwörter im Voraus generieren.

In dem System, demgegenüber man sich authentifizieren soll, wird der letzte so bestimmte Wert als Anfangswert gespeichert. Bei der Authentifizierung gibt der Benutzer den vorletzten berechneten Wert ein. Das System wendet darauf die Einwegfunktion an und vergleicht das Ergebnis mit dem gespeicherten Wert. Stimmen beide überein, ist der Benutzer authentifiziert. Der gerade eingegebene Wert wird als neuer Vergleichswert gespeichert. Bei jeder Runde gibt der Benutzer das höchste noch nicht verwendete Paßwort ein. Jedes Paßwort wird so nur einmal verwendet.

Der Nachteil dieses Verfahrens liegt darin, daß die Liste generiert und der letzte Wert unverfälscht an das System übermittelt werden muß, das die Überprüfung durchführen soll. Wenn alle Paßwörter aufgebraucht sind, muß eine neue Liste generiert werden. Es eignet sich deshalb nicht für häufige und kurzlebige Authentifizierung.

¹⁵³ vgl. [sch96-1] Abschnitt 8.1

7.2.4 Einseitige und gegenseitige Authentifizierung

In den meisten heutigen Authentifizierungsverfahren muß eine Seite der anderen ihre Echtheit beweisen. Der umgekehrte Beweis ist nicht vorgesehen. Beispielsweise gibt ein Bankkunde beim Abheben am Geldautomaten zusammen mit seiner Karte seine PIN preis. Aber woher weiß er, daß der Geldautomat nicht manipuliert wurde und heimlich die Daten seiner Karte zusammen mit der PIN abspeichert? Er kann es nicht wissen, er muß dem Automaten vertrauen.

Hier dient die Authentifizierung nur dazu, unechte Kunden (mit gestohlenen oder gefälschten Karten) festzustellen.

Damit beide Seiten sicher sein können, müssen sie sich gegenseitig ihre Echtheit beweisen: Beim Einsatz von Prozessorchipkarten statt Magnetkarten kann auch der Geldautomat der Karte seine Echtheit beweisen, bevor diese ihr Geheimnis preisgibt.

Es gibt spezielle Verfahren, die gleichzeitig beide Kommunikationspartner authentifizieren.¹⁵⁴

7.3 Authentifizierungsmöglichkeiten im ISDN

Im ISDN kann die Authentifizierung an verschiedenen Stellen eingesetzt werden. Benutzer können sich gegenüber Endgeräten, Vermittlungsstellen oder anderen Benutzern authentifizieren; Netzeinrichtungen können dies gegenüber Endgeräten oder anderen Netzeinrichtungen tun. Diese Einsatzgebiete werden jetzt der Reihe nach beschrieben.

7.3.1 Authentifizierung innerhalb einer TK-Anlage

Innerhalb einer ISDN-TK-Anlage treten verschiedene Stellen miteinander in Beziehung, um eine Kommunikation intern oder extern aufzubauen. Um vor Manipulationen sicher zu sein, kann man die Stellen ihre Identität beweisen lassen.

Die Berechtigungen innerhalb einer TK-Anlage sind durch die Programmierung den einzelnen Endgeräten zugewiesen. Die Endgeräte werden meistens mit Personen assoziiert, stehen aber auch jedem Anderen offen. Jeder Benutzer eines Telefons verfügt über die Rechte, die das Telefon hat. Oft wäre es aber sinnvoller, wenn Rechte personengebunden vergeben werden könnten. Dazu müßten sich die Benutzer gegenüber einem beliebigen Endgerät authentifizieren.

Das kann sogar so weit gehen wie in den Mobilfunknetzen: Der Benutzer verfügt über eine an ihn gebundene Chipkarte. Nur er kennt die PIN zum aktivieren der Karte. Sobald die Karte in ein beliebiges Mobiltelefon eingelegt und die passende PIN eingegeben wird, ist diesem Telefon die personengebundene Rufnummer zugewiesen. Dazu gehören auch benutzerspezifische Einstellungen wie Anrufbeantworter und Rufumleitungen und Berechtigungen wie Fax- und Datendienst.

Auch ISDN-Endgeräte könnten so arbeiten. Dazu müßten sie allerdings mit einem Chipkartenleser ausgestattet werden. Im Zuge zunehmender Mobilisierung des Festnetzes¹⁵⁵ werden solche Karten in Zukunft eingesetzt werden. Bis dahin könnte man Benutzerkennungen und Paßwörter vergeben, mit denen sich die Benutzer an den Endgeräten anmelden können. Dazu müßte lediglich die Software der Geräte (Firmware) angepaßt werden.

¹⁵⁴ Ein Überblick findet sich in [sch96-1], Abschnitte 3.2 und 3.3.

¹⁵⁵ vgl. [sai97-2]

Auch die Endgeräte selbst können sich bei der nächst höheren Instanz, der TK-Anlage authentifizieren. Damit kann man ausschließen, daß nicht berechtigte oder gar manipulierte Endgeräte angeschlossen werden. Und wenn Endgeräte mit Chipkartenlesern zum Einsatz kommen, kann so verhindert werden, daß alte Geräte ohne diese Sicherheitseinrichtung weiterhin verwendet werden.

Als zusätzliche Sicherheit können umgekehrt auch die Anlage gegenüber dem Endgerät und das Endgerät gegenüber dem Benutzer beweisen, daß sie echt sind und nicht manipuliert wurden.

Zwischen Anlage und Endgerät kann man dasselbe Verfahren einsetzen wie in umgekehrter Richtung. Zwischen Endgerät und dem Benutzer selbst ist das nicht möglich. Hier kann aber der Einsatz von Chipkarten abhelfen: Das Endgerät kann der Chipkarte als Stellvertreter des Benutzers seine Echtheit beweisen. Wenn der Benutzer seine Karte ständig bei sich trägt, wird er ihr eher vertrauen als einem beliebigen Endgerät.

7.3.2 Authentifizierung im D-Kanal

Über den D-Kanal können sich Endgeräte und Vermittlungsstelle gegenseitig authentifizieren. Die Vermittlungsstelle weiß ohnehin, über welchen physikalischen Anschluß (port) ein Datenpaket eintrifft. Mit Hilfe der Authentifizierung kann sie aber auch sicher gehen, daß das Paket vom berechtigten Endgerät am Ende der Leitung stammt und nicht durch ein aufgeklebtes Gerät eines Angreifers eingeschleust wurde. Das Endgerät kann dadurch umgekehrt sicher sein, mit der Vermittlungsstelle zu kommunizieren und nur ihr die Daten der B-Kanäle anzuvertrauen und nicht einem Angreifer, der sich in die Leitung geschaltet hat.

Im analogen Telefonnetz gibt es bereits einen vergleichbaren Ansatz:

Nachdem 1995 zahlreiche überhöhte Telefonrechnungen auftraten und die Anschlußhaber sich weigerten zu zahlen, wurde der Ruf nach manipulationssicheren Anschlüssen laut. Die Telekom entwickelte daraufhin eine Telefondose¹⁵⁶ mit integriertem Authentifizierungs-Chip und passende Gegenstücke für die Vermittlungsstellen. Mit ihrer Hilfe kann bewiesen werden, daß ein Gespräch nicht nur über die Leitung eines Teilnehmers sondern sogar über seine Telefondose, also aus seinen Räumen heraus stattgefunden haben muß. Damit scheiden Angriffe auf die Leitung zwischen Vermittlungsstelle und dem Übergabepunkt aus.

Dem Autor liegen aber Informationen vor, daß es sich um funktionslose „Dummies“ gehandelt hat. Dennoch hat der Placebo-Effekt offensichtlich gewirkt. Nicht zuletzt nach Einführung der Einzelgesprächsnachweise ist es um angeblich überhöhte Rechnungen ruhig geworden.

7.3.3 Authentifizierung im ZGS-7

Auch die Vermittlungsstellen untereinander vertrauen sich zur Zeit blind. Dazu gehören die Teilnehmervermittlungsstellen in der Ortsebene und die Fernvermittlungsstellen des darüberliegenden Fernnetzes. Hinzu kommen die Netzübergänge zu anderen Netzen (in Deutschland zunächst einmal zum nationalen Netz)¹⁵⁷ und die zentralen Datenbanken des intelligenten Netzes (IN).

¹⁵⁶ TAE - Telefon-Anschluß-Einheit

¹⁵⁷ vgl. Abschnitt 4.4.6

Das ermöglicht einige Angriffe auf das Telekommunikationsnetz eines Betreibers, wie sie in Kapitel 4 beschrieben sind. Auch hier kann an Sicherheit gewonnen werden, wenn sich die Vermittlungsstellen gegenseitig ausweisen müssen.

Wie bei der Verschlüsselung gibt es auch eine abschnittsweise und eine Ende-zu-Ende-Authentifizierung.

Die Nachrichten, die der Steuerung und insbesondere dem Routing einer Nutzkanalverbindung dienen, müssen in jedem Knoten ausgepackt und in den oberen Schichten ausgewertet werden. Die Knoten erzeugen gegebenenfalls neue Pakete, die sie an den nächsten Knoten weitersenden. Deshalb reicht es, wenn sich die Netzknoten nur gegenüber ihren unmittelbaren Nachbarn ausweisen.

Wie im Kapitel über Verschlüsselung erwähnt, gibt es im ZGS-7 auch Pakete, die transparent zum Ende durchgereicht werden. Sie enthalten aber auch Routing-Informationen, die in jedem Knoten ausgewertet werden müssen. Deshalb bietet sich eine Mischform von Ende-zu-Ende und abschnittsweiser Authentifizierung an: Die Adreßinformationen werden von den Zwischenstationen neu erzeugt. Hier ist also die abschnittsweise Authentifizierung gefragt. Die eigentliche Nutzinformation hingegen wird erst vom Empfänger ausgewertet. Deshalb bietet sich dafür die Ende-zu-Ende-Authentifizierung an.

7.3.4 Ende-zu-Ende-Authentifizierung

Auch eine Ende-zu-Ende Authentifizierung der Kommunikationspartner ist möglich. Dafür stehen wahlweise der B-Kanal oder der D-Kanal zur Verfügung:

Der B-Kanal wird transparent von einem Kommunikationspartner zum anderen durchgeschaltet. Eine Ende-zu-Ende Authentifizierung der beiden Kommunikationspartner ist deshalb in einer hohen Protokollebene leicht zu implementieren.

Dafür ist am Markt bereits Soft- und Hardware verfügbar. Die sicherheitsbedürftigen Anwender können diese Lösungen unabhängig von ihrem Netzbetreiber installieren und verwenden. Von Nachteil ist aber, daß alle Anwender, die miteinander gesichert kommunizieren wollen, dieselbe Lösung verwenden müssen. Da es hier keine Standards gibt, sind die angebotenen Produkte in der Regel nicht zueinander kompatibel.

Die Authentifizierung über den D-Kanal ist da schon schwieriger aber konzeptuell sauberer. Denn alle die Verbindung steuernden Daten gehören in den D-Kanal. Da hier aber bisher keine Protokollelemente für die Authentifizierung vorgesehen sind, wäre eine Protokolländerung nötig. Für eine kleine Lösung vorab könnte man bisher unbenutzte, optionale Protokollelemente benutzen. Diese Authentifizierung funktioniert dann aber nur innerhalb eines Netzes.

Bei der Integration der Authentifizierung in die genormten Protokolle kann sie als Zusatzleistung allen interessierten Anschlußinhabern angeboten werden. Inkompatibilitäten werden so von vorn herein vermieden.

Wie bei der Verschlüsselung¹⁵⁸ ergibt sich auch hier ein Problem mit Konferenzschaltungen, das eine Sonderbehandlung verlangt: Es sind mehr als zwei Kommunikationspartner beteiligt, die auch getrennt authentifiziert werden müssen. Damit nun nicht jeder jedem anderen Konferenzteilnehmer seine Echtheit beweisen muß, könnte man den Konferenzleiter zu einer Person des allgemeinen Vertrauens machen. Er authentifiziert sich gegenüber allen Teilnehmern, die er in die Konferenz aufnimmt und alle Teilnehmer gegenüber

¹⁵⁸ siehe Abschnitt 6.5.4

ihm. Gleichzeitig kann ein gemeinsamer Sitzungsschlüssel für alle Beteiligten vereinbart werden, mit dem die Nutzkanäle verschlüsselt werden.

7.4 besondere Anforderungen des ISDN an die Authentifizierung

7.4.1 Allgemeine Anforderungen

Für die Anwendung im ISDN kommen nur asymmetrische Authentifizierungsverfahren in Frage. Symmetrische Verfahren sind auf einen sicheren Kanal zum Austausch der Schlüssel angewiesen. Damit eignen sie sich nicht für spontane Kommunikation zwischen beliebigen Teilnehmern der weltweiten Telekommunikationsnetze.

Die asymmetrischen Verfahren sind auf vertrauenswürdige zentrale Instanzen angewiesen, die die öffentlichen Schlüssel aller Teilnehmer bereitstellen. Sie müssten in den Netzen eingerichtet werden und die Daten aller ISDN-Teilnehmer weltweit bereithalten. Um die Antwortzeiten kurz zu halten müssten sie in jedem Netz mehrfach in replizierter Form existieren. Das wiederum bedingt eine sichere Kommunikation über ZGS-7-Netze zwischen den Instanzen zum Abgleich der Daten.

Alle Benutzer müssen diesen Instanzen vertrauen. Sie stellen damit auch einen zentralen Angriffs- und Schwachpunkt der gesamten Sicherheit im System dar. Denn wer in einer solchen Instanz gefälschte öffentliche Schlüssel einspielt, der kann die Identität eines beliebigen anderen Teilnehmers annehmen.

Außerdem müssen die in Frage kommenden Verfahren Zufallszahlen und Zeitstempel einsetzen, um gegen replay-Attacken sicher zu sein:

7.4.2 Bei Ende-zu-Ende-Authentifizierung

Eine Ende zu Ende Authentifizierung läßt sich entweder über den durchgehenden B-Kanal oder über die Steuerverbindung via D-Kanal und ZGS-7 implementieren:

Eine Ende-zu-Ende-Authentifizierung über den D-Kanal und das Zeichengabenetz läßt sich nur als zusammengesetzte abschnittsweise Authentifizierung realisieren. Denn es gibt keinen durchgehenden Steuerkanal von einem Ende der Kommunikationsbeziehung zum anderen. Statt dessen müssen sich so der Benutzer bzw. das Endgerät und die Ortsvermittlungsstelle gegenseitig authentifizieren, dann die Ortsvermittlungsstelle und die erste Fernvermittlungsstelle und so weiter bis zur Zielvermittlungsstelle und von dort zum Zielteilnehmer.

Das ist aber nicht gleichbedeutend mit einer echten Ende-zu-Ende-Authentifizierung, bei der sich die beiden Kommunikationspartner gegenseitig überprüfen. Durch die vielen zwischengeschalteten Stationen läßt sich bei diesem Verfahren auch an vielen verschiedenen Stellen betrügen.

Hinzu kommt, daß das D-Kanal-Protokoll und das Zeichengabesystem 7 zur Zeit keine Protokollelemente für die Authentifizierung enthalten. Sie müssten beide erweitert werden. Zum D-Kanal-Protokoll hat R. Sailer an der Universität Stuttgart einen konkreten Vorschlag gemacht.¹⁵⁹ Er wird im Abschnitt 7.4.3 näher beschrieben.

Die Authentifizierung über den B-Kanal kommt ohne Protokolländerungen aus. Hier ist sogar noch nicht einmal die Unterstützung durch den Netzbetreiber erforderlich. Schon heute können deshalb im B-Kanal Ende-zu-Ende-Authentifizierungsverfahren eingesetzt

¹⁵⁹ vgl. [sai97-2]

werden. Dazu müssen lediglich die verwendeten Endgeräte der Kommunikationspartner für eine Authentifizierung gerüstet sein. Im Fall von Rechnerkommunikation mit Hilfe einer ISDN-Karte ist das recht einfach in der Treiber- oder Anwendungssoftware zu implementieren. Telefone und andere Endgeräte werden Authentifizierung und Verschlüsselung in Zukunft auch unterstützen.

7.4.3 Bei Authentifizierung zwischen Benutzer und Netz

Für eine Authentifizierung zwischen den Teilnehmern beziehungsweise deren Endgeräten und dem Netz kommt nur der D-Kanal in Frage. Denn der B-Kanal wird in der Vermittlungsstelle transparent durchgeschaltet und nicht ausgewertet.

R. Sailer an der Universität Stuttgart schlägt vor, das D-Kanal-Protokoll um einige Elemente zu erweitern:

Beim Eintreffen der setup-Nachricht in der Vermittlungsstelle wendet diese sich an die zentrale Schlüsseldatenbank. Mit Hilfe des dort erhaltenen öffentlichen Schlüssels überprüft sie die Identität des A-Teilnehmers. Bei Erfolg wird dem B-Teilnehmer eine setup-Nachricht mit der Identität von A geschickt. Der A-Teilnehmer ist also schon mit dem ersten Klingelzeichen bei B authentifiziert. Der B-Teilnehmer führt dann seine Chipkarte in sein Endgerät ein. Daraufhin wird auch er authentifiziert. Bei Erfolg bekommt der A-Teilnehmer eine Quittung, die ihm anzeigt, daß die Authentifizierung erfolgreich war und es bei B klingelt. Sobald B das Gespräch annimmt, wird die Verbindung mit einer connect-Nachricht durchgeschaltet. Falls die Authentifizierung fehlschlägt, wird der Verbindungsaufbau abgebrochen;¹⁶⁰ als Auslösegrund wird das neue Element „authentication failed“ gesendet.

Zur Verdeutlichung ein Ablaufschema:¹⁶¹

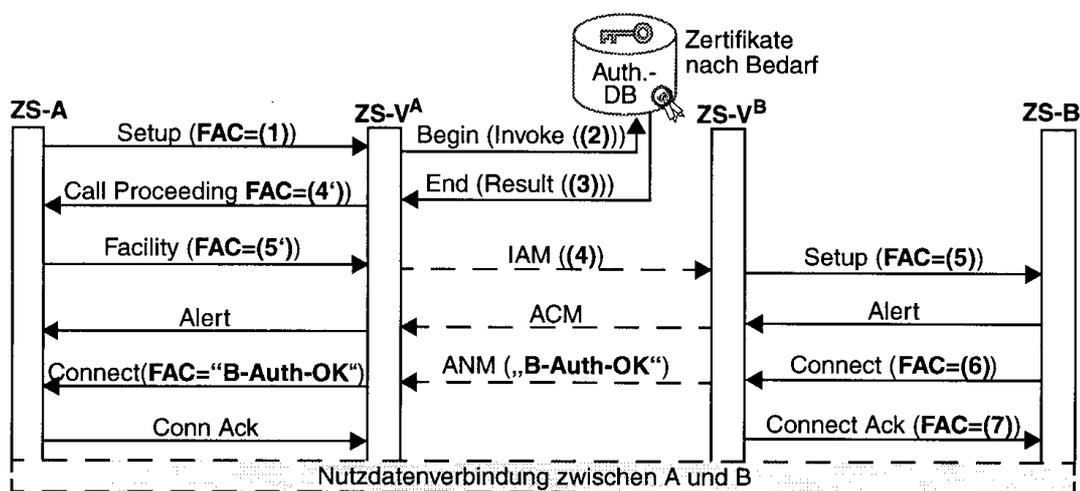


Abbildung 1.9: Integration der Nachrichten in die Verbindungssignalisierung im (N-) ISDN

7.5 Eignung/Anpassung bekannter Verfahren

Aus den Ausführungen der vorangegangenen Abschnitte geht hervor, daß symmetrische Authentifizierungsverfahren für die Anwendung im ISDN nicht geeignet sind.

¹⁶⁰ wie bei einem besetzten Anschluß oder inkompatiblen Endgeräten.

¹⁶¹ aus [sai97-2]

Unter der Voraussetzung, daß zentrale vertrauenswürdige Instanzen zur Verwaltung der öffentlichen Schlüssel eingerichtet werden, lassen sich asymmetrische Verfahren sehr gut einsetzen.

Um die Authentifizierung und auch die verschlüsselte Kommunikation für die Teilnehmer zu vereinfachen, bietet sich der Einsatz von Chipkarten an. In ihnen wird der geheime Schlüssel des Benutzers gespeichert. Vor einer Kommunikation wird die Chipkarte in das Endgerät gesteckt, das wiederum die Authentifizierung beim Netz durchführt. Auf diesem Wege wird auch ein Sitzungsschlüssel vereinbart, mit dem die eigentliche Kommunikation symmetrisch verschlüsselt werden kann.

Der Einsatz von Chipkarten wird kommen, was aber bedingt, daß alle Endgeräte über einen Chipkartenleser verfügen. Bis dahin können Übergangslösungen nach dem gleichen Prinzip¹⁶² eingesetzt werden.

¹⁶² asymmetrische Authentifizierung mit Schlüsselvereinbarung für die spätere symmetrische Verschlüsselung der Nutzdaten

8 Firewalls

8.1 Einleitung

Die vorangegangenen Kapitel befaßten sich mit der Frage, wie man die Sicherheit im ISDN durch den Einsatz kryptographischer Methoden verbessern kann. In diesem Kapitel geht es darum, wie sich manche Sicherheitslücken auch ohne diese Mittel schließen lassen.

Das Konzept der firewalls ist heute aus dem Internet bekannt. Die Metapher basiert auf Feuerschutzwänden (firewalls), die in Gebäuden an ganz bestimmten Stellen gezielt eingebaut werden, um verschiedene Bereiche voneinander so abzutrennen, daß bei einem Brand in einem Bereich die angrenzenden Bereiche jenseits der Schutzmauer nicht in Mitleidenschaft gezogen werden.

Beim Einsatz von elektronischen firewalls in Computer- und Kommunikationsnetzen verfolgt man dasselbe Ziel: Aneinander angrenzende Bereiche sollen voneinander getrennt werden, um die Sicherheit zu erhöhen. Alles, was in einem Bereich Schaden anrichten könnte und aus einem anderen Bereich stammt, wird abgeblockt.

Dieses Kapitel untersucht die Einsatzmöglichkeiten von Firewalls im ISDN. Als diensteintegrierendes Telekommunikationsnetz hat das ISDN viele Gemeinsamkeiten mit dem Internet. Deshalb wird zunächst der firewall-Ansatz des Internet beschrieben und dann auf die verschiedenen Einsatzgebiete im ISDN übertragen.

8.2 Firewalls im Internet

Mit zunehmender Verbreitung des Internet und mit steigenden Rechner- und Benutzerzahlen stieg auch das Sicherheitsbedürfnis. Etwa 1994 wurde deshalb das firewall-Konzept für die Anwendung im Internet aufbereitet. Seitdem wächst die Zahl der eingesetzten Produkte stetig.

8.2.1 Funktionsweise

Eine Firewall agiert als Filter. Zwei Netzbereiche werden über genau einen Übergang (Gateway) miteinander verbunden.¹⁶³ Dieser Übergang kann die Aufgabe der Firewall übernehmen. Dann werden alle Pakete in beiden Richtungen analysiert, bevor sie weitergeleitet werden. Unzulässige Pakete werden verworfen. Dabei kann nach Absender- oder Empfängeradresse oder auch nach dem Inhalt der Pakete gefiltert werden.

Im Internet werden Firewalls üblicherweise verwendet, um Firmennetze an das globale Netzwerk anzuschließen. Damit wird zum einen den Mitarbeitern Zugriff auf das gesamte Internet gewährt und zum anderen können selbst Daten für den Abruf durch Geschäftspartner und Interessenten bereitgestellt werden.

Bei einer solchen Firewall zwischen einem Firmennetz und dem Internet kann man verschiedene Paketfilter sinnvoll einsetzen, je nach der Richtung, in der die Daten fließen:

¹⁶³ Wegen der besseren Ausfallsicherheit können auch mehrere Gateways existieren. Sie müssen dann alle nach den gleichen Regeln filtern.

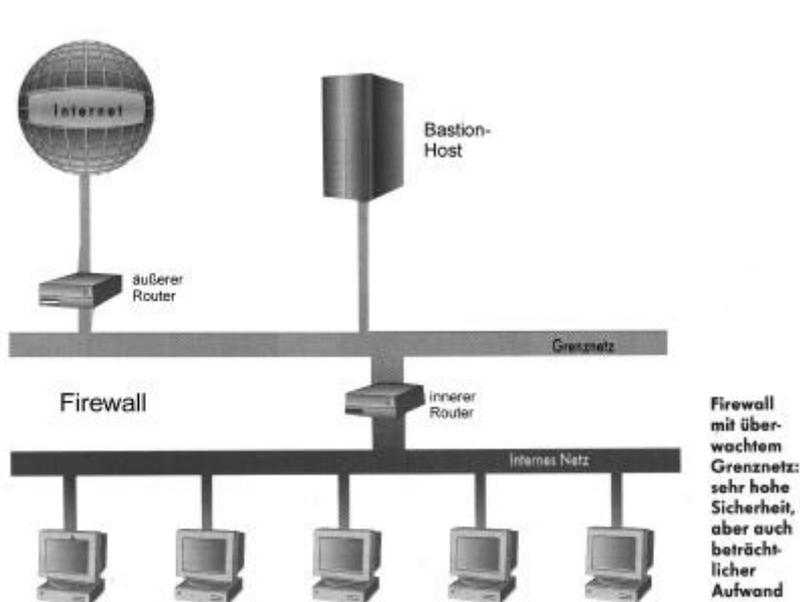
Eingehende Datenpakete können nur für tatsächlich existierende Empfänger (IP-Adressen)¹⁶⁴ entgegengenommen werden. Außerdem kann man die möglichen Absender der Datenpakete einschränken: Entweder empfängt man Daten nur von einem festen Kreis vertrauter Rechner oder man schließt besonders wenig vertrauenswürdige aus.

Auch für ausgehende Datenpakete kann man besonders unsichere Empfänger ausschließen oder nur bestimmte zulassen. Man kann auch festlegen, daß nur bestimmte Rechner Daten an Empfänger außerhalb des eigenen Netzbereichs schicken dürfen. Damit lassen sich beispielsweise öffentliche Terminals im Besucherbereich eines Unternehmens nicht für anonyme e-mails mißbrauchen.

Außerdem können Datenpakete nach ihrem Inhalt gefiltert werden. Damit kann man einen Rechner zum Beispiel nur für bestimmte Dienste öffnen. Alle externen Rechner dürfen dann zwar prinzipiell auf ihn zugreifen, aber eben nur für bestimmte Dienste.

Die Kombination aus diesen Regeln ermöglicht eine sichere und flexible Konfiguration eines Netzwerks. Das Regelwerk wird aber schnell sehr komplex und dadurch schwer zu überblicken. Das birgt die Gefahr in sich, daß sich ein Unternehmen für sicher hält, aber eine schwerwiegende Lücke im Abwehrmechanismus übersehen hat.

Damit ein Teil der Daten im Firmennetz intern und extern zur Verfügung stehen kann, ohne daß darunter die Sicherheit der Daten leiden muß, installiert man am besten eine zweistufige Firewall:



aus: c't 4/97 Seite 312

Zwischen den beiden Routern sind die Rechner angesiedelt, auf die sowohl aus der Firma heraus als auch von Außen zugegriffen werden soll. Dazu gehören zum Beispiel Webserver oder Loginserver für Außendienstmitarbeiter. Hinter dem inneren Router befindet sich das gesamte restliche Firmennetz.

Der äußere Router läßt nur Pakete nach innen, die an einen der Rechner im Zwischenetz gerichtet sind. Alle anderen Pakete werden herausgefiltert. Nach außen können aber alle Pakete passieren, die für irgendeinen Rechner außerhalb des Firmennetzes bestimmt sind. Der innere Router läßt keinerlei Pakete durch, die von Außenherb kommen. Es ist

¹⁶⁴ Im Internet werden alle Rechner weltweit eindeutig durch ihre IP-Adresse (4 Bytes) adressiert

nur für Pakete der eigenen Rechner im Zwischennetz durchlässig. Nach Außen können dagegen alle Pakete passieren.

8.2.2 Betriebsmodi

Es gibt zwei grundsätzliche Philosophien für den Einsatz einer Firewall: Entweder ist alles erlaubt, was nicht ausdrücklich verboten ist oder es ist alles verboten, was nicht ausdrücklich erlaubt ist.

Unter Sicherheitsaspekten ist es besser, alles zu verbieten, was nicht ausdrücklich erlaubt ist. Das kann aber gerade bei der Einführung neuer Dienste und Merkmale zu Problemen führen, weil diese erst freigegeben werden müssen. Flexibler aber weniger sicher ist es, alles zu erlauben, was nicht ausdrücklich verboten ist. Das wiederum führt aber zu Problemen, wenn neu entdeckte Sicherheitslücken nicht sofort geschlossen werden. Über sie ist dann ein ungehinderter Zugriff durch die Firewall hindurch möglich.

Beim Filtern nach Absender- oder Empfängeradressen oder dem Inhalt von Paketen kann es zu Widersprüchen kommen. Einem Rechner kann prinzipiell erlaubt sein, auf einen anderen zuzugreifen, aber der Zugriff auf einen bestimmten Dienst kann grundsätzlich verboten sein. Auch hier muß man sich für eine Sicherheitsphilosophie entscheiden:

Man kann alles zulassen, was nicht von allen Regeln verboten wird oder alles verbieten, was von mindestens einer Regel verboten wird. Die sicherere Variante ist es, alles zu verbieten, sobald dadurch eine Regel verletzt würde. Sie schränkt aber auch gleichzeitig am stärksten ein.

8.2.3 Produkte

Firewalls für das Internet gibt es sowohl als Hard- als auch als Softwarelösung. Die Softwarelösung ist preiswerter, eignet sich aber nur für kleinere Netzsegmente, da sie einen geringeren Datendurchsatz erreicht als Hardware. Die Software wird auf einem Rechner mit zwei Netzwerkkarten installiert. Jede Karte ist an ein Netzwerksegment angeschlossen. Bevor Datenpakete aus dem einen in das andere Netzwerksegment geschickt werden, prüft die Software sie nach den oben beschriebenen Regeln. Unzulässige Pakete werden verworfen, zulässige über die andere Netzwerkkarte in das Zielsegment geleitet.

8.2.4 Problem IP-Spoofing

Die derzeitige Version des Netzwerkprotokolls TCP/IP hat keine ausreichenden Sicherheitsmechanismen. Insbesondere sieht sie keine starke Authentifizierung vor. Es ist leicht, Datenpakete mit gefälschter Absenderadresse zu erzeugen, um firewalls zu überlisten. Diesen Angriff nennt man „IP-Spoofing“.

Er macht die oben beschriebenen Filterung der Absenderadresse nutzlos, da ein Angreifer lediglich eine IP-Adresse eines vertrauten Rechners vortäuschen muß.

Das Problem läßt sich weitgehend dadurch lösen, daß man im äußeren Gateway sehr restriktiv filtert. Dann können zwar gefälschte Anfragen nach Innen gelangen, die eigentlich interessanten Antworten nach Außen bleiben aber im Gateway hängen.

8.3 Firewalls im ISDN

Im ISDN bietet es sich an, alles zu verbieten, was nicht ausdrücklich erlaubt ist. Denn hier treten Änderungen am Protokoll nur selten auf und es ist die sicherere Variante.

Firewalls lassen sich - wie oben beschrieben - jeweils am Übergang zwischen zwei getrennten Bereichen einsetzen. Daraus ergeben sich folgende Einsatzgebiete im ISDN:

- in einer ISDN-TK-Anlage am Übergang vom öffentlichen zum Firmennetz
- in den Vermittlungsstellen am Übergang von der Teilnehmeranschlußleitung zum Nutz- und Steuerkanalnetz eines Netzbetreibers
- im ZGS-7-Netz eines Netzbetreibers am Übergang zum nationalen Netz und dort am Übergang zum internationalen Netz.

Sie werden in den folgenden Abschnitten beschrieben.

8.4 Firewalls in ISDN-TK-Anlagen

Für die Sicherheit innerhalb einer ISDN-TK-Anlage ist der Betreiber selbst verantwortlich. In Kapitel 2 wird eine Reihe von Schwachstellen in solchen Anlagen beschrieben und Angriffe gezeigt, die diese Schwachstellen ausnutzen.

8.4.1 Firewall im D-Kanal

Viele Anlagen verwenden intern zusätzliche Protokollelemente im D-Kanal. Sie sind in der internationalen D-Kanal-Spezifikation nicht enthalten und steuern anlageninterne Leistungsmerkmale. Ein Angreifer kann in Kenntnis des verwendeten Anlagentyps solche Protokollelemente von Außen erzeugen und beispielsweise einen Raum abhören, indem er das Mikrofon des darin befindlichen Telefons aktiviert.

Mit Hilfe von Firewalls kann man Angriffe abblocken, die von außen über den D-Kanal kommen, indem alle international nicht spezifizierten Protokollelemente durch eine D-Kanal-Firewall gefiltert werden, wenn sie von außen kommen.

Auch ausgehende D-Kanal-Pakete kann man durch die Firewall prüfen lassen. Damit lassen sich Verbindungen zu bestimmten, nicht vertrauenswürdigen Anschlüssen verhindern. Außerdem können verbotene Datenübertragungen im D-Kanal (user-to-user-signalling¹⁶⁵) erkannt und verhindert werden. Ohne diese Hilfe wäre es Innentätern leichter möglich, geheime Daten telefonisch nach Außen zu transportieren.

Zur Zeit werden in der Industrie erste D-Kanal-Firewalls entwickelt. Sie werden frühestens 1998 am Markt verfügbar sein.

8.4.2 Absichern des Fernwartungszugangs

Angriffe über den Fernwartungszugang umgehen die Firewall, weil sie als normale Datenverbindungen über einen B-Kanal zu einer Nebenstelle in der TK-Anlage aufgebaut werden. B-Kanäle werden transparent durchgeschaltet und nicht verarbeitet, so daß sie auch kritische Befehle für die Anlagenprogrammierung enthalten können. Um den Fernwartungszugang abzusichern, kann man die in Abschnitt 2.7.1.1 beschriebenen Mittel verwenden oder aber die Anlagensoftware so entwerfen, daß sie bestimmte kritische Befehle über einen Fernwartungszugang nicht annimmt. Hier sind die Anlagenhersteller gefordert.

Ein solches Vorgehen kommt einer Firewall im Fernwartungszugang gleich.

¹⁶⁵ siehe Abschnitt 3.9.7

8.5 Firewalls in Vermittlungsstellen

8.5.1 Schutz vor Angriffen über Teilnehmerleitungen

Auch der Betreiber eines Telekommunikationsnetzes muß sich vor Angriffen von Seiten der Teilnehmer schützen. Hier ist ebenfalls der D-Kanal als Steuerkanal der kritischste Punkt. Wie in Kapitel 3 beschrieben, läßt sich auch die Vermittlungsstellensoftware von außen über den D-Kanal eines beliebigen Anschlusses angreifen.

Die Netzbetreiber verwenden deshalb an den Teilnehmeranschlüssen ebenfalls Filter für die D-Kanal-Befehle, die in ihrer Funktionalität einer Firewall gleichkommen.

Sie prüfen beispielsweise die übermittelte Rufnummer des Anrufers bei einem Verbindungsaufbau. Nur wenn es sich um eine der Nummern handelt, die diesem Anschluß zugewiesen sind, wird sie weitergeleitet. Andernfalls wird sie mit einer gültigen Rufnummer des Anschlusses überschrieben.

Die Aufgaben der Filter sind bereits in den ETSI-Standards für den D-Kanal festgelegt. Dort gibt es zu jedem Protokollelement einen Anhang, in dem beschrieben wird, wie das Element aufgebaut ist und welche Fehler gefiltert werden müssen. Dazu gehören beispielsweise zu lange oder zu kurze Daten zu einem Befehl u.ä.

Ein Angreifer kann sich aber diese Standards besorgen und sieht genau, welche Pakete gefiltert werden. Wenn das Protokoll eine Lücke enthält, kann er sie für seinen Angriff ausnutzen. Dieser Schutz bietet deshalb keine echte Sicherheit, weil quasi die Konfiguration der Firewall offenliegt.

8.5.2 Schutz vor Angriffen über das Zeichengabenetz

Auch aus Richtung des Zeichengabenetzes lassen sich die Vermittlungsstellen angreifen. Es ist zwar schwieriger, erst einmal in das Zeichengabenetz hineinzukommen, dann ist ein Angriff auf beliebige Vermittlungsstellen eines Netzbetreibers aber leicht. Denn die Vermittlungsstellen sind gegen das Zeichengabenetz nicht abgesichert. Sie vertrauen ihm blind.

Hier ließe sich die Sicherheit durch den Einsatz von Firewalls ebenfalls erhöhen. Alle eingehenden Pakete, die nicht dem Standard entsprechen oder für Angriffe geeignet sind, könnten gefiltert werden. Darüber hinaus wäre es an dieser Stelle sinnvoll, in einer der vorhandenen Überwachungseinrichtungen des AcceSS-7-Systems¹⁶⁶ Alarm auszulösen, sobald kritische Pakete erkannt wurden.

8.6 Firewalls im Zeichengabenetz

8.6.1 In den Zeichengabepunkten

Die Zeichengabepunkte sind in den meisten Fällen Vermittlungsstellen. Sie vertrauen den anderen Knoten des Zeichengabenetzes. Zum Schutz der Vermittlungsstellen vor Angriffen aus dem Zeichengabenetz können wie oben beschrieben eingehende Nachrichten in den Vermittlungsstellen gefiltert werden. Außerdem können in den Vermittlungsstellen alle in Richtung Zeichengabenetz ausgehenden Nachrichten gefiltert werden. Alle Pakete,

¹⁶⁶ siehe Abschnitt 4.6.4

die nicht den Normen entsprechen oder im Verdacht stehen, Schaden anzurichten werden verworfen. Auch hier kann optional Alarm in einer Kontrollstelle ausgelöst werden.

8.6.2 An den Netzübergängen

An den Übergängen der Zeichengabenetze wird bereits gefiltert. Die in Abschnitt 4.4.4 beschriebenen Gateways zwischen den Netzen der einzelnen Netzbetreiber und dem nationalen Netz sowie zwischen den nationalen Netzen und dem internationalen Netz übernehmen neben dem routing der Zeichengabepakete diese Aufgabe. Pakete, die nicht dem Standard entsprechen werden nicht in das Zielnetz weitergeleitet sondern verworfen. So schützen die einzelnen Netzbetreiber ihre Telekommunikationsnetze vor Angriffen aus anderen, möglicherweise weniger gut geschützten Netzen.

Hier ist es ebenfalls sinnvoll, die Pakete nicht nur zu verwerfen, sondern eine Überwachungsstelle zu informieren. Solche Überwachungsstellen gibt es ohnehin in den Zeichengabenetzen. Sie sind stets über die Auslastung und die Funktionsbereitschaft der einzelnen Netzbereiche informiert. Wenn Sie zusätzlich auch von allen gefilterten Paketen Kenntnis erhalten, können sie deren Ursprung ermitteln und gegen sich so gegen weitere Angriffe aus dieser Richtung noch besser schützen.

Ein so entdeckter Angreifer muß sich zumindest andere Wege suchen, um sein Opfer weiterhin attackieren zu können.

Zwischen den Netzen verschiedener Netzbetreiber ist das Filtern aber nur dann möglich, wenn ein nationales Transitnetz existiert. In Deutschland ist das der Fall, viele andere Länder verzichten aber darauf. Dazu gehören auch die USA. Hier sind alle Zeichengabernetze der zahlreichen Netzbetreiber eng miteinander vermascht. Das macht die Implementierung von Filtern schwierig.¹⁶⁷

¹⁶⁷ siehe Abschnitt 4.4.6

Literaturverzeichnis

- [alb90] Albensöder, A. [Hrsg]:
Netze und Dienste der Deutschen Bundespost Telekom
v.Decker's Verlag, Heidelberg, 2. Auflage, 1990
- [arn92] Arnold, Ulrich:
Heterogene Netzwerke: erfolgreiche Lösungen zur Vernetzung von unterschiedlichen Rechnern und Betriebssystemen
Franzis, 1992
- [avm94] **CAPI 2.0** Spezifikation + addendum
AVM, Berlin, 1994
- [ban95] Bandow, Gerhard, u.a:
Zeichengabesysteme: Eine neue Generation für ISDN und intelligente Netze
L.T.U. Vertriebsgesellschaft, Bremen, 2. Auflage 1995
- [bei95] Beitzke, Dietrich:
Am Scheideweg, ISDN - richtig umsatteln
in c't (Heise Verlag) 5/95 p. 220ff
- [bin92] Binder, Ulrich [u.a.]:
Telekommunikations-Anlagen in ISDN-Technik
expert-Verlag, Ehningen, 1992
- [bla95-1] Blab, Herbert; SIEMENS:
Siemens HiCom, Mitbestimmung und Datenschutz
Siemens München 1995
- [bla95-2] Blab, Herbert; SIEMENS:
Hoher Sicherheitsstandard bei Hicom
in: Siemens telecom report 18/1995
- [blü93] Blümel, Bernd; Kuhle, Bernd:
Effiziente Unternehmenskommunikation mit ISDN
v. Decker-Verlag, Heidelberg, 1993
- [boc86] Bocker, Peter:
ISDN - Das diensteintegrierende digitale Nachrichtennetz - Konzepte, Verfahren, Systeme
Springer Verlag, Heidelberg, 1986
- [boe95] Boesen, Albert; Meilen, Matthias; Kötz, Wilfried:
ISDN-Referenzhandbuch
Thomson Publishing International, 1995
- [bra95] Brauer, Kai:
Rundumversorgung - ISDN-Kommunikation leichtgemacht
in c't (Heise Verlag) 8/95 p. 72ff
- [bsi94] BSI - Bundesamt für Sicherheit in der Informationstechnik
Gefährdung und Sicherheitsmaßnahmen beim Betrieb von digitalen Telekommunikationsanlagen
Köln, Bundesanzeiger 4/1994
- [bsi95] BSI - Bundesamt für Sicherheit in der Informationstechnik:
IT-Grundschutzhandbuch: Massnahmenempfehlungen für den mittleren Schutzbedarf
Köln, Bundesanzeiger 1995
- [con95] controlware Schulungsunterlagen:
Euro-ISDN - der Weg von 1TR6 zu DSS-1
controlware Schulungszentrum, Dietzenbach, 1995

- [dbt94] Deutsche Bundespost Telekom:
Das ISDN-Anwenderhandbuch, 62 innovative Lösungen aus Wirtschaft und Verwaltung
Verlag Hoppenstedt, Darmstadt, 1994
- [dib90] Dibold, H:
Intelligente Netze - Einführung und Grundlagen
in: Der Fernmeldeingenieur, 4/90, Heidecker-Verlag, Nürnberg
- [ehl84] Ehlers, Stephan; u.a.:
Telekommunikation: Dienste, Übersichten, Entscheidungshilfen
Verlag Technik, 1. Auflage 1984
- [els91] Elsing, Jürgen:
Das OSI-Schichtenmodell: Grundlagen und Anwendungen der X.200
IWT-Verlag, 1. Auflage 1991
- [fei96] Feichtinger, Herwig:
Wegbereiter, jedem Dienst sein Protokoll
in c't (Heise Verlag) 3/96 p. 126ff
- [gam94] Gamm, Christoph von; Ungerer, Bert:
Baustein der Zukunft, ATM wird LAN und WAN vereinen
in c't (Heise Verlag) 10/94 p. 138ff
- [göl97] Göller, Joachim:
Der ISDN-D-Kanal im Dialog
Elektronik-Praktiker-Verlag, 1997
- [got95] Gottschalk, H; Gotthardt, B:
Zeichengabesystem Nr. 7, Stabilität und Sicherheit, Einsatz eines Monitorsystems
in: Der Fernmeldeingenieur, 11+12/95, Heidecker-Verlag, Nürnberg
- [ham89] Hammer, Volker; Pordesch, Ulrich; Roßnagel, Alexander:
Gestaltungsanforderungen für die ISDN-Nebenstellenanlage der Hochschulregion Darmstadt
provet - Projektgruppe verfassungsverträgliche Technikgestaltung, Darmstadt, 1989
- [ham90] Hammer, Volker; Pordesch, Ulrich; Roßnagel, Alexander:
Prüfung des rechtsgemäßen Betriebs von ISDN-Anlagen
provet - Projektgruppe verfassungsverträgliche Technikgestaltung, Darmstadt, 1990
- [ham93] Hammer, Volker; Pordesch, Ulrich; Roßnagel, Alexander:
Betriebliche Telefon- und ISDN-Anlagen rechtsgemäß gestaltet
Springer-Verlag, Berlin, Heidelberg, 1993
- [hau96] Haugh, John H:
Toll Fraud and Telabuse, a multibillion Dollar national Problem
Pasha Publications, Inc, Arlington, Virginia, USA, 2nd edition 1996
- [heg92] Hegering, Heinz-Gerd; Läßle, Alfred:
Ethernet: Basis für Kommunikationsstrukturen; Grundlagen - Realisierung - Betrieb
DATACOM-Verlag, 1992
- [itu93] ITU-T:
Digital Subscriber Signalling System No.1 (DSS-1) - ISDN User-Network Interface Layer 3 - Specification for Basic Call Control
ITU-Recommendation Q.931
- [kaf] Kafka, Gerhard [Hrsg]:
Erfolgreiche Vernetzung mit ISDN
Interest Verlag, Augsburg (Loseblattsammlung)
- [kah92] Kahl, Peter [Hrsg]:
ISDN: das neue Fernmeldenetz der Deutschen Bundespost Telekom
v. Decker-Verlag, Heidelberg, 4. Auflage 1992

- [klu92] Klug, Wolfgang:
OSI-Vermittlungsdienst und sein Verhältnis zum ISDN-D-Kanal-Protokoll - Spezifikation und Analyse mit Produktnetzen
Gesellschaft für Mathematik und Datenverarbeitung (GMD), Bonn, 8/1992
- [köh93] Köhntopp, Kristian:
Einheitliche Sicht - Netzwerkprotokolle im Internet
in c't (Heise Verlag) 3/93 p. 232ff
- [kos96-1] Kossel, Axel:
Digitale Vorteile - von ISDN profitieren
in c't (Heise Verlag) 3/96 p. 102ff
- [kos96-2] Kossel, Axel:
Innere Sicherheit
in c't (Heise Verlag) 10/96 p. 332ff
- [kow95] Kowalski, Bernd:
Security Management System - SMS
in: Der Fernmeldeingenieur, 4+5/95, Heidecker-Verlag, Nürnberg
- [luc97-1] Luckhardt, Norbert:
Schwer entflammbar
In c't (Heise Verlag) 4/97 p. 308ff
- [luc97-2] Luckhardt, Norbert; Schmidt, Jürgen:
Trau, schau, wem!
In c't (Heise Verlag) 6/97 p. 308ff
- [met93] Metzendorf, H. Vorlesungsmanuskript **ISDN**
Fachhochschule der Telekom, Dieburg, 1993
- [mor91] Moritz, Peter:
Einstieg ins Zukunftsnetz, Computerbasierte Kommunikation im ISDN
in c't (Heise Verlag) 11/91 p. 70ff
- [mor93] Moritz, Peter:
ISDN-Aufgelöst - Fähigkeiten und Grenzen des digitalen Netzes
in c't (Heise Verlag) 8/93 p. 100ff
- [mor94] Moritz, Peter:
Autobahn-Baustelle - Die Daten-Highways der Telekom
in c't (Heise Verlag) 10/94 p. 102ff
- [mor95] Moritz, Peter:
Richtig auf Draht - Sparen bei der Telekommunikation
in c't (Heise Verlag) 4/95 p. 314ff
- [mor96] Moritz, Peter:
Info-Adern, Breitbandangebote der Telekom
in c't (Heise Verlag) 3/96 p. 290ff
- [muh94] Muhl, W; Stolz, H:
Sicherheitsarchitekturen und -konzepte für Telekommunikationsnetze
in: Der Fernmeldeingenieur, 6+7/94, Heidecker-Verlag, Nürnberg
- [mül91] Müller, Franz:
Standardisierung in der Telekommunikation
in: c't (Heise Verlag) 3/91 p. 327ff
- [ost96] Ostheimer, Frank:
ISDN Prüftelefon 93i
in: Deutsche Telekom, Unterrichtsblätter, Juli 1996, p350ff
- [por91] Pordesch, Ulrich; Hammer, Volker; Roßnagel, Alexander:
Prüfung des rechtsgemäßen Betriebs von ISDN-Anlagen
Vieweg-Verlag 1991

- [rei95] Reif, Holger
Netz ohne Angst
in c't (Heise Verlag) 9/95 p. 174ff
- [ros93] Rost, Martin; Schack, Michael:
DFÜ - ein Handbuch: Recherchen in weltweiten Netzen
Heise-Verlag, 1993
- [sai96-1] Sailer, Reiner:
Integrating Authentication into Existing Protocols
5th Open Workshop On High Speed Networks, Paris, 3/96
- [sai96-2] Sailer, Reiner; Kühn, P. J.:
Ein Domain-Konzept zur systematischen und wirtschaftlichen Integration von Sicherheit in Kommunikationsnetze
in: it + ti Informationstechnik und Technische Informatik, 38. Jg., Heft 4, 1996, pp 30-33
- [sai97-1] Sailer, Reiner:
Authentikation als Grundlage der Skalierung von Sicherheit in der Kommunikationstechnik
in: Zitterbart, M (Hrsg.) Tagungsband Kommunikation in verteilten Systemen 1997
Springer Verlag 2/97, pp 62-76
- [sai97-2] Sailer, Reiner, Kühn, P. J.:
Integration von Authentikationsverfahren in Kommunikationsnetze unter Verwendung separat sichtbarer Bereiche
in: Müller, G; Pfitzmann, A. (Hrsg.) Mehrseitige Sicherheit in der Kommunikationstechnik
Addison Wesley, 7/97
- [sch90-1] Schröder, Hartmut:
ISDN-Endgerät PC (Teil 1: Integration einer ISDN-Karte im PC)
in c't (Heise Verlag) 10/90 p. 325ff
- [sch90-2] Schröder, Hartmut:
ISDN-Endgerät PC (Teil 2: Steuerung mittels D-Kanal-Protokoll)
in c't (Heise Verlag) 11/90 p. 240ff
- [sch92] Schremmer, Stefan:
ISDN-D-Kanal-Protokoll der Schicht 3, Spezifikation und Analyse mit Produktnetzen, Arbeitspapiere der GMD 640
Gesellschaft für Mathematik und Datenverarbeitung (GMD), Bonn, 4/1992
- [sch96-1] Schneier, Bruce:
Angewandte Kryptographie
Addison-Wesley, 1996
- [sch96-2] Schoblick, Robert:
ISDN-Installations- und Servicehandbuch
Franzis-Verlag, München, 2. Auflage 1996
- [stö95] Stöttinger, Klaus:
X.25-Datenpaketvermittlung
Datacom-Verlag, 2. Auflage 1995
- [thc97] The Hacker's Choice:
Spaß mit Sept, 1997. In The Hacker's Choice Magazine No.4
Im Internet: <http://merlin.koeln-net.com/~plasmoid/thc/>
- [tie93] Tierling, Eric:
Fernverbindung - mit ISDN von LAN zu LAN
in c't (Heise Verlag) 10/93 p. 76ff
- [tzs92] Tzschach, Hans; Haßlinger, Gerhard:
Codes für den störungssicheren Datentransfer
Oldenbourg-Verlag 1993

- [wac93] Wachholz, G:
Euro-ISDN, die europäische Version der ISDN Der Telekom
in: Der Fernmeldeingenieur, 11/93, Heidecker-Verlag, Nürnberg
- [wil93] Wilde, Michael; Zivadinovic, Dusan:
ISDN-Schau, Hard- und Software für die digitale Kommunikation
in c't (Heise Verlag) 8/93 p. 112ff
- [ziv96] Zivadinovic, Dusan:
Tele-Zauber, Trends der Telekommunikation
in c't (Heise Verlag) 4/96 p. 148ff

